WILLKIE FARR & GALLAGHER LLP
BENEDICT HUR (SBN 224018)
bhur@willkie.com
SIMONA AGNOLUCCI (SBN 246943)
sagnolucci@willkie.com
EDUARDO SANTACANA (SBN 281668)
esantacana@willkie.com
TIFFANY LIN (SBN 321472)
tlin@willkie.com
One Front Street, 34th Floor
San Francisco, California 94111
Telephone: (415) 858-7400
Facsimile: (415) 858-7599

Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JOHN DOE I, et al., individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No. 3:23-cv-02431-VC
Consol. w/ 3:23-cv-02343-VC

DEFENDANT GOOGLE LLC'S OPPOSITION TO PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION; MOTION TO DISMISS

Date: July 20, 2023
Time: 2:00 p.m.
Ctrm.: 2, 4th Floor

Complaint Filed: May 17, 2023

District Judge Vince Chhabria
San Francisco Courthouse, Ctrm. 4

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. INTRODUCTION

Plaintiffs' 160-page, 560-paragraph Consolidated Amended Complaint ("CAC") and its 255 pages of declarations fail under their own weight and cannot support the extraordinary preliminary relief Plaintiffs seek. In an effort to plead around the host of case law in this District rejecting similar kitchen-sink pleadings, Plaintiffs offer a tangle of contradictory allegations and ignore that it is developers who place the relevant cookies on Plaintiffs' devices, not Google.

Websites and apps, including those of healthcare providers, use a variety of products like Google Analytics ("GA"), to analyze users' experiences on their properties. Their use is widely understood, dutifully disclosed, and regularly consented-to by users. This District has repeatedly recognized that developers have the right to employ analytics tools, and that the providers of those tools are mere vendors to the developer. And while Plaintiffs claim a fundamental incompatibility of analytics software and healthcare, the U.S. Department of Health & Human Services ("HHS") itself acknowledges that healthcare website developers may use analytics tools in compliance with the Health Insurance Portability and Accountability Act ("HIPAA"). After all, analytics providers only provide developers with information about how users use the developers' own properties—information the companies could analyze in-house, but choose instead to analyze using a third-party service. Without any legal basis, and resting on a host of unsupported allegations, Plaintiffs' Motion asks this Court to ban health care providers from using such tools in their entirety.

Plaintiffs' Motion meets none of the requirements for a preliminary injunction. Every one of the *Winter* factors weighs against an injunction. ***First,*** Plaintiffs are unlikely to succeed on the merits for the following reasons: **(1)** it is *developers*, not Google, who intentionally incorporate GA code into their app or website; **(2)** Google's GA Terms of Service ("TOS") require developers to disclose their use of cookies and, where required, obtain consent for their use, and each website in question here does so; **(3)** none of the information the websites allegedly sent to GA included any personally identifying information ("PII"), personal health information ("PHI"), or health details about any person in particular; **(4)** Google prohibits using sensitive health information to target advertising. In fact, Plaintiffs do not even allege they received any targeted ads following their use of the websites in question. Further, Google makes no attempt to connect health

information to the identity of any particular Google user. While Plaintiffs assert that Google *could* tie the data it receives to re-identify users, they provide no evidence that Google ever does so. Finally, **(5)** under HIPAA, developers who are Covered Entities are responsible for obtaining a Business Associate Agreement ("BAA") from any vendor to whom they will send PHI. Google makes clear that it does not offer or enter into BAAs in connection with GA. Accordingly, if a HIPAA-regulated entity cannot ensure that it will avoid sending GA any PHI, the entity cannot incorporate GA into its website or app.

Second, Plaintiffs cannot show that they would suffer any harm, let alone irreparable harm, without a preliminary injunction. Plaintiffs have stopped using the websites in question, and the alleged harm is purely speculative, particularly given that Google does not collect PII or PHI.

Third, the balance of the equities and the public interest do not support Plaintiffs' motion. The injunction would harm the Health Care Providers who rely on GA and other tools to analyze their own data and to make healthcare more accessible and cost-efficient, without harming anyone's privacy interests. And it would pose an enormous burden on Google. By contrast, the injunction would not affect Plaintiffs, who no longer use the Websites.

Finally, the Motion should be denied because Plaintiffs do not and cannot describe the relief sought or the grounds for relief with specificity. Fed. R. Civ. P. 65(d)(1)(B)–(C).

Plaintiffs' Motion is nothing more than an improper attempt to have this Court consider and impose a remedy for an alleged HIPAA violation, which only the Secretary of HHS has the discretion to impose (and which is meritless anyway), without hearing from the very Health Care providers who will be most affected. The Court should deny Plaintiffs' Motion, including the request to provisionally certify a class in order to grant this relief that Plaintiffs have no standing to request and that much of the proposed provisional class would surely oppose.

II. ISSUES TO BE DECIDED

The issues are: (i) whether Plaintiffs seek a mandatory injunction subject to a heightened burden; (ii) whether Plaintiffs meet the factors necessary for a preliminary injunction; (iii) whether Plaintiffs describe the relief sought and the grounds for relief with sufficient specificity; (iv) whether provisional class certification is appropriate; and (v) whether Plaintiffs state a claim.

III. BACKGROUND

A. Statement of Facts

Plaintiffs allege that healthcare websites and apps transmitted Plaintiffs' and other users' sensitive health information to Google without Plaintiffs' consent, and that Google profited from that information through marketing, ad targeting, and product improvement. CAC ¶¶ 1–6.

Plaintiffs assert the following claims against Google: Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.* ("ECPA" or the "Wiretap Act") (Count 1); Violation of the California Invasion of Privacy Act, Cal. Penal Code. § 630, *et seq.* ("CIPA") (Count 2); Invasion of Privacy, Cal. Const. art. I, § 1 (Count 3); Intrusion Upon Seclusion (Count 4); Violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 ("UCL") (Count 5); Trespass to Chattels (Count 6); Statutory Larceny, Cal. Penal Code § 496 (Count 7); California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502 ("CDAFA") (Count 8); Aiding and Abetting (Count 9); Breach of Express Contract (Count 10); Breach of Implied Contract (Counts 11 and 12); Good Faith and Fair Dealing (Count 13); and Unjust Enrichment (Count 14). Plaintiffs' Motion for Preliminary Injunction and Provisional Class Certification ("Motion") relates to Counts 1, 2, 4, and 5. Mot. at 1.

1. Google Provides Products Developers May Use To Help Their Companies.

Website and app developers use a variety of products to analyze users' experiences on their properties and to market their companies, including Google products like Google Analytics ("GA"), Google Tag Manager ("GTM"), Google Ads, and Google Display Network ("Display").

GA is one of many available products that developers may choose to integrate into their properties. Decl. of Steve Ganem ("Ganem Decl.") ¶ 5. Google tags are lines of code used for analysis and advertising that developers may incorporate into their websites. *Id.* ¶ 6. GTM is a tag management system that allows developers to deploy GA tags on their properties. *Id.* ¶ 7. Google Ads is a service companies may use to assist in marketing. *Id.* ¶ 17. Google Ads is separate from GA; only developers who use *both* Google Ads and GA, and link their two accounts, may then use their *own* GA data in service of their *own* advertising—subject to Google's restrictions. *Id.* ¶ 18.

Display is a third, separate product that has no relevance to Plaintiffs' allegations.

Developers use Display to sell advertising space on their websites to advertisers; it does not use GA data for personalized advertising. Decl. of Oscar Takabvirwa ("Takabvirwa Decl.") ¶ 31.

2. GA Is a Measurement Tool Developers May Integrate Into Websites and Apps.

Analytics tools like GA allow companies, including health care providers, to improve their online presence by expanding accessibility, understanding their visitors' needs, and predicting demand.[1] Decl. of Mark Teehan ("Teehan Decl") ¶ 14-18. The American Hospital Association recently emphasized the importance of these technologies to "allow hospitals to actually reach more patients and expand access to underserved communities." *Id.* Ex. 1.

Plaintiffs assert that Google deploys its source code on health care provider websites. Mot. at 1. That is false, as Plaintiffs' counsel well know. Counsel for Plaintiffs have brought multiple lawsuits against health care providers regarding the same alleged conduct at issue here. In four of those matters, Plaintiffs' counsel filed preliminary injunction motions relying on similar declarations from Dr. Timothy Libert and Richard M. Smith. Each motion failed. But in those motions, the plaintiffs made clear (when it suited them) that it is *health care providers* who deploy GA code on their websites and apps, not Google.[2]

To deploy the GA code, the developer must first create a GA account and consent to Google's Terms of Service ("TOS"), and the policies incorporated therein. Ganem Decl. Ex. 3. The developer may then integrate the freely available Google tag or GA Software Development Kit ("SDK") into their website or app's code, all without any cooperation, involvement,

[1] Ganem Decl. ¶ 4. The current version of GA is called GA4. The prior version of GA for web is called Universal Analytics ("UA"), and the prior version of GA for apps is Google Analytics for Firebase ("GA4F"). *Id.*

[2] *See* Request for Judicial Notice ("RJN") Ex. 1 ¶ 15 (*Doe v Partners Healthcare System, Inc.*, Case No. 1984-CV-01651 (Suffolk County, Massachusetts)) (*"Defendants intentionally deploy computer source code* at their web properties . . ."); Ex. 2 at 3 (*Doe v. Sutter Health*, Case No. 34-2019-00258072-CU-BT-GDS (Sacramento County, California)) ("HTML s*ource code deployed by Sutter* . . . These re-directed HTTP requests to third-parties are *funneled by Sutter* . . ."); Ex. 4 at 11 (*Doe v. Virginia Mason Medical Center*, Case No. 19-2-26674-1 SEA (King County, Washington)) ("Plaintiff's injuries were *caused by Virginia Mason's deployment of source code*. . ."); Ex. 9 at 1 (*Doe v. Medstar Health, Inc., et al.*, Case No. 1:23-cv-01198-JRR (D. Md. May 5, 2023)) (seeking a preliminary injunction prohibiting "*Medstar and Cerner from deploying source code* that deposits third-party cookies") (all emphases added).

participation, or even human contact with Google. *Id.* ¶¶ 6–7. Developers may choose to use GTM to deploy the GA tag on their website or app. GTM does not collect any user data and does not send any data to GA beyond what the GA tag itself collects. *Id.* Google does not have access to or control over the code developers use. *Id.*

Cookies are small pieces of text sent to a user's browser when visiting a website. They serve a range of purposes including personalization, keeping users signed in, and preventing fraud. Zervas Decl. Appx. C ¶ 2. Cookies may use "cookie values," typically a randomly generated string of characters, to associate browsing activity by the same user across multiple browsing sessions if the user visits in the same browser, on the same device, and has not cleared cookies. *Id.* First-party cookies belong to the developer that placed the code creating them into the website. First-party cookie values are set by the website a user is currently visiting. Only the website that created the cookie's value can access it. Third-party cookies are set by a domain other than the website the user is currently visiting and can only be accessed by the outside creator-domain. *Id.* ¶ 29 & Appx. C ¶¶ 4–7. Third-party cookies can therefore log user preferences across websites. *Id.* Users can block cookies, though this may interfere with a website's functionality. Zervas Decl. ¶ 102. Developers may use GA code to generate their own first-party cookie values to collect user engagement data on their website and report aggregated site usage statistics without PII. *Id.* ¶ 40; Ganem Decl. Ex. 19. Google does not "disguise" GA cookies as first-party cookies. CAC. ¶ 53; Mot. 19. The cookies in the GA code that developers choose to incorporate into their websites belong to the developers, not Google, and cannot track users across different websites. Zervas Decl. ¶ 30, 39–41. The cookie value can only be accessed by the website the user is visiting, and is meaningless to other websites and third-party services. *Id.* They *are* first-party cookies. *Id.*

Further, developers who implement GA choose which data to collect—subject to Google's restrictions. Ganem Decl. ¶ 9. Under Google's policies and the developer's settings, GA logs only certain user interactions automatically, called standard web or app events. *Id.* ¶ 24 & Ex. 14. Standard events are basic interactions such as opening an app or updating the operating system. *Id.* ¶ 25. Developers may also choose to enable "enhanced measurement," which includes basic user events like downloading a file or clicking on a link. *Id.* ¶ 26 & Ex. 15. None of the standard

events provide PII to Google or any information that could be categorized as "health information" or "sensitive" information, even if the developer has enabled enhanced measurement. For instance, while Plaintiffs identify URLs as "communications" and "Health Information," it is developers who determine whether the page URL is recorded with the event, or whether to change the data recorded by overriding the "page_location" parameter. *Id.* Ex. 14. For example, "first_visit" is triggered when users first visit a website or launch an app. *Id.* ¶ 25. It does not provide Google any information about what the user saw or did after opening the website or app. *Id.* Likewise, the enhanced measurement option "form_submit" only tells developers when a user submits a form; it does not contain any information about what is in the form. *Id.* Ex. 15. And, of course, developers design the URL's text in the first place, not Google. Zervas Decl. ¶¶ 40 n. 89, 69 n. 147.

Developers may also create and define custom events to suit their particular needs. Ganem Decl. ¶ 27 & Ex. 16. Custom events are unique to an individual app or website. Because developers define these events independently, Google has no insight into, and makes no effort to decipher, the meaning of a given event (e.g., a custom event called "Medstar_event" means no more to Google than a custom event called "custom_event_1"). *Id.* ¶ 28. Developers may also choose to enable the collection of more comprehensive event data, such as location data and URLs. *Id.* ¶¶ 23, 26. Developers, not Google, control these settings.

Developers also choose whether and which data to share with Google. *Id.* ¶ 9. Unless developers enable the "data sharing with Google" setting, Google processes the data only as required to provide and maintain the GA service. *Id.* ¶ 29 & Ex. 17.

3. Google Implements Numerous Safeguards Against Receiving PII.

Developers may analyze patterns in user engagement using identifiers (strings of characters that allow developers to distinguish between users and devices), which are collected with certain events. *Id.* ¶ 9. The default identifiers are all pseudonymous, not personally identifiable. *Id.* ¶ 31. Contrary to Plaintiff's allegations (Mot. at 4, 5; CAC. ¶¶ 59, 79, 91, 170), GA4 never logs user IP addresses.[3] Ganem Decl. ¶ 36 & Ex. 20.

[3] UA, the prior version of GA, allowed developers to request masking of IP addresses. Ganem Decl. ¶ 36. Regardless, UA did not associate IP addresses with any specific individuals.

For example, the Google Advertising ID ("AdID"), or the Apple iOS equivalent Identifier for Advertisers ("IDFA"), is a pseudonymous, device-specific string of characters that is neither tied to a user's identity nor used to personally identify a user. *Id.* ¶ 33. Users may reset their AdID at any time. *Id.* "Client IDs" are randomly generated alphanumeric strings stored in the browser's cookies, allowing developers to determine whether website visits were made by the same user. *Id.* ¶ 34 & Ex. 18. Client IDs cannot identify users across the websites and apps of different businesses, and are not associated with specific individuals. *Id.* A user may reset their Client ID at any time by, for example, clearing their browser's cookies. *Id.*

Unless both the user (if she is a signed-in Google account holder) and developer affirmatively enable specific settings, identifiers are pseudonymized and limited to the visitor's session on the particular developer's property. (Google has no way of tying non-user data to identifying information in a Google account.) *Id.* ¶ 38. Google allows users to save their activity to their Google Account ID ("GAIA ID") if the user enables four Google Account settings: (1) Web & App Activity ("WAA"); (2) a supplemental WAA setting ("sWAA"), allowing Google to associate activity on third-party websites and apps with the user's Google Account; (3) Google Ads Personalization ("GAP"); and (4) New Ad Control ("NAC"), allowing users to tailor the ads they view based on the saved account activity. *Id.* ¶¶ 39–40. sWAA and NAC are disabled by default and require affirmative opt-in from the user. Zervas Decl. ¶ 84.

By enabling all four settings, a user can choose to save their browsing history and app activity to their Google Account, as long as the developer has enabled another optional setting, Google Signals ("Signals"). Zervas Decl. ¶ 43, 84. Once such activity is saved to the user's Google account, the user can view and manage their saved activity on their My Activity page. Ganem Decl. ¶ 44. Developers can enable Signals to measure user interactions across devices, for example, if a logged in Google user visits a site using their phone and computer. *Id.* ¶ 55. If a user is not signed in, *or* has not turned on any one of the four functions, *or* visits a website or app that has not enabled Signals, only pseudonymous data is collected and it cannot be linked across devices or to a specific user. Ganem Decl. ¶¶ 41–42.

Google further ensures data cannot be used to identify a specific user by employing

sophisticated encryption techniques and redaction. *Id.* ¶¶ 43–48. GA uses multiple servers, each of which receive segmented data and employ separate encryption schemes, to check user consent. *Id.* 44–46. If the user is not signed in, or has not enabled any one of the consent settings, only pseudonymous data is used. *Id.* ¶ 42.

Even for users that have enabled all four settings, Google ensures their data still cannot be "joined" or combined with any pseudonymous data. Google does so by removing overlapping identifiers, creating slight errors or "fuzziness" in the data, and encrypting the logs using separate, short-term decryption keys. *Id.* ¶¶ 48–49. After the keys are deleted, decryption is impossible. *Id.* Google additionally protects all GA data by storing it only for limited durations. *Id.* ¶ 49. And Google strictly limits access to the data. Google employees cannot see any identifiers without receiving specific, short-term access permission. *Id.* ¶ 50.

4. Google Prohibits Developers from Sharing PII Or PHI with Google.

In order to use GA, Google requires that developers consent to and abide by the GA TOS. *Id.* ¶ 11 & Ex. 3. The TOS require developers to, among other things, (1) disclose their use of GA including "how it collects and processes data;" (2) disclose their use of cookies; (3) obtain user consent as required by law; and (4) refrain from transmitting data to Google that Google could recognize as PII:

> You will not and will not assist or permit any third party to pass information, hashed or otherwise, to Google that Google could use or recognize as personally identifiable information . . . You must post a Privacy Policy and that Privacy Policy must provide notice of Your use of cookies, identifiers for mobile devices (e.g., Android Advertising Identifier or Advertising Identifier for iOS) or similar technology used to collect data. You must disclose the use of Google Analytics, and how it collects and processes data. . . . You will use commercially reasonable efforts to ensure that a User is provided with clear and comprehensive information about, and consents to, the storing and accessing of cookies or other information on the User's device . . . .

Id. Google instructs developers to, among other things, "remove PII from user-entered information before it is sent to Analytics," ensure website URLs and titles are free from PII, and take special care when naming custom dimensions. *Id.* If developers discover they have accidentally sent Google PII, Google provides tools to delete the prohibited data from their accounts. *Id.* ¶ 14.

Further, Google prohibits developers from using GA in a way that would violate HIPAA or create any responsibilities *for Google* under HIPAA. *Id.* ¶ 15 & Ex. 7. HIPAA applies to a Covered Entity (generally, healthcare providers) and business associates ("a person who […] on behalf of such covered entity […] creates, receives, maintains, or transmits protected health information" or "[p]rovides […] legal, actuarial, accounting, consulting, data aggregation […], management, administrative, accreditation, or financial services for such covered entity […]"). *See* 45 C.F.R. §§160.102, 160.103. Under HIPAA, developers who are Covered Entities are responsible for obtaining a BAA from any vendor to whom they will send PHI. *See* 45 C.F.R. §164.308(b)(3), 164.314(a). Google is not a business associate and neither offers to nor enters into BAAs in connection with the relevant services. Ganem Decl. ¶ 16. Accordingly, if a HIPAA-regulated entity cannot ensure that it will avoid sending GA any PHI, the entity cannot use GA. *Id.* This includes, among other things, refraining from using GA on pages that are HIPAA-covered or collecting data that may be considered PHI. *Id.*

Plaintiffs name six healthcare provider web domains: Kaiser Permanente ("Kaiser"), MedStar Health ("Medstar"), Mercy Medical Center in Baltimore, MD ("MD Mercy"), Gundersen Health System ("Gundersen"), Mercy Hospital, and OSF HealthCare; and one health insurance web domain, United Healthcare ("UHC") in their Motion (together, the "Websites"). Mot. Notice at 2. Each discloses its use of cookies to collect information and their use of third-party tools. Zervas Decl. ¶ 92–96.

5. Google Prohibits The Use Of Sensitive Health Information In Personalized Advertising.

Google does not allow personalized advertising based on sensitive health information, including "[p]hysical or mental health conditions, including diseases, sexual health, and chronic health conditions," and "[p]roducts, services, or procedures to treat or manage chronic health conditions." Ganem Decl. Exs. 10, 12. If an advertiser violates Google's Advertising Policies, Google may block their ads, disable certain advertising features, or suspend an advertiser's Google Ads account. Zervas Decl. ¶ 70.

Developers who have both GA and Google Ads accounts may choose to link their accounts

and use certain of their GA data with their Google Ads. *Id.* ¶ 18 & Ex. 8. However, the use of their data is restricted based on how the website or app is classified in the Google Ads system. Google Ads classifies a web domain as "Sensitive" based on the website's text; apps are classified based on the app's Play Store or iOS store description. Both of which are created by developers. Takabvirwa Decl. ¶ 4. The sensitivity classification determines whether the property can use certain personalized advertising features. *Id. at* ¶ 6. Google's policies do not allow advertisers and developers to use sensitive health information for remarketing or personalized advertising. Zervas Decl. ¶¶ 49, 52–53, 56.

6. Google Does Not Passively Bar The Use Of Sensitive Information For Personalized Advertising; It Proactively Prevents It.

Google Ads' sensitivity classifications govern whether developers may use data from their properties for remarketing and personalized advertising with Google advertising platforms, such as Google Search, Display Ads, and YouTube.[4] *Id.* ¶ 75; Takabvirwa Decl. ¶¶ 6, 10.

Health care providers are generally classified as Sensitive in the Google Ads system. Takabvirwa Decl. ¶¶ 6, 9, 27. Sensitive websites and apps cannot use advertiser-curated audience lists, or "remarketing lists" (advertising lists based on who has engaged with their web properties). *Id.* ¶ 10 & Ex 1. Further, GA and Google Ads data from Sensitive websites and apps cannot be used for personalized advertising by the Google Ads system. If a website or app has a mix of sensitive and non-sensitive content, Google considers them "Mixed Content" and allows them to build advertiser-curated audience lists, but ads targeted at those audiences are manually reviewed to prevent sensitive ads from being served to those audiences. *Id.* ¶ 19.

All of the Websites, except UHC's, are classified as Sensitive or Mixed Content for the purpose of building audience lists. *Id.* ¶ 7. All of the Websites, except UHC's, are classified as Sensitive for the purpose of personalized advertising by Display Ads. Health insurance providers like UHC are generally not considered Sensitive for purposes of building audience lists or

[4] Google Ads classifies websites *internally*; the page Plaintiffs repeatedly cite, *see, e.g.*, Mot. at 7; CAC ¶ 193 (citing https://developers.google.com/adwords/api/docs/appendix/verticals), is a deprecated page used by Google's deprecated AdWords Application Programming Interface ("API"), a separate product unrelated to GA. GA does not determine which, if any, of its developers are health care providers. Ganem Decl. ¶ 51.

personalized advertising in Display Ads. *Id.* ¶¶ 26–27, 31. All of the Websites are classified as Sensitive (or Not Found - meaning they are not used) for the purpose of personalized advertising by the Google Search and YouTube platforms. *Id.* ¶ 26, 28–30.

7. Plaintiffs Present Irrelevant And Misleading "Evidence" That Does Not Support Their Claims.

Plaintiffs' Motion rests on an unverified complaint and anecdotal expert declarations. *See In re Meta Pixel Healthcare Litig.*, 2022 WL 17869218, at *20 (N.D. Cal. Dec. 22, 2022) (classifying a similar declaration of Richard M. Smith as "anecdotal."). The only allegation Plaintiffs provide any evidence for is that some healthcare providers use GA—an undisputed fact Google requires developers to disclose. *See* Ganem Decl. Ex. 3. Plaintiffs jump to the conclusion that all healthcare provider websites that use GA are necessarily in violations of HIPAA (and, by definition, Google's own policies). Plaintiffs offer no evidence to support this broad conclusion, nor do they explain why Google would be liable for those websites' alleged HIPAA violations.

The Smith Declaration (Dkt. 42-1)—which Plaintiffs rely on exhaustively—shows only that some websites use GA. In contrast to Smith's Declaration in *In re Meta Pixel*, 2022 WL 17869218, at *3, Smith does not (and cannot) show that he received *any* targeted advertising from Google after visiting these properties, much less targeted advertising based on PHI. Nor does Smith show that any websites shared *any* identifying information with Google, or that any GA data was used for any purpose other than the website's own analytics. Zervas Decl. ¶¶ 134.

Dr. Timothy Libert's Declaration (Dkt. 42-2) ("Libert Decl.") is similarly misleading and equally void of substance.[5] All Dr. Libert shows is, again, that some websites use GA and GTM to collect site usage information. He does not show that Google received PHI, or that the data was used for anything other than the websites' own analytics. *Id.* ¶ 126

Dr. Zubair Shafiq's Declaration (Dkt. 42-4) ("Shafiq Decl.") uses a non-credible and inaccurate entropy analysis to claim that Google can *theoretically* combine pieces of information

[5] Google has concurrently moved the Court for an order disqualifying Dr. Timothy Libert from serving as an expert witness for Plaintiffs due to his recent prior employment as a privacy engineer at Google, where he worked closely with in-house counsel to develop systems and policies relating to cookie privacy and compliance.

to identify users. Dr. Shafiq relies on the false premise that the information transmitted to Google, such as screen size, color depth, and screen resolution, are sufficiently independent so that they can be combined to provide more information than is otherwise present in each attribute. In reality, many of these attributes overlap, and therefore provide much less information than Dr. Shafiq assumes. *Id*. ¶¶ 143–46. Further, Dr. Shafiq neglects that many of the data points he alleges can be used to personally identify users (such as IP address) can be dynamic, shared among many individuals, and reset. *Id.* ¶¶ 141–42. Regardless, he does not allege that Google actually combines any data to identify users. At most, Dr. Shafiq merely claims that Google theoretically *could* use complex algorithmic techniques to link together data. In actual practice, Google uses complex encryption techniques and technical safeguards to ensure that data is not identifiable. Ganem Decl. ¶¶ 43–50.

8. Plaintiffs Knowingly Bring Moot Claims.

Plaintiffs use the Medstar website as a "case example" throughout their Motion, but their injunction request regarding Medstar is moot. Plaintiffs' counsel represent a proposed class in Maryland against Medstar based on the same conduct and claims Plaintiffs allege here. *See Doe I v. Medstar Health, Inc.*, No. 1:2023-cv-01198 (D. Md. May 5, 2023). There, Plaintiffs' Counsel also filed a preliminary injunction motion seeking to "prohibit[] MedStar . . . from deploying source code that deposits third-party cookies for marketing purposes." RJN Ex. 9 at 1. On July 6, 2023—before Plaintiffs filed their Motion here—Plaintiffs' counsel entered into a stipulation with Medstar agreeing that Medstar would cease use of Google services *inside* its patient portal (but not other parts of its website outside the portal) and that the plaintiffs' preliminary injunction motion thus "is moot."[6] RJN Ex. 10. Plaintiffs thus illustrate their Motion with moot claims.

[6] Google is aware of three other preliminary injunction motions Plaintiffs' Counsel have filed in cases against health care providers; none have succeeded. *See* n.3, supra; *Doe v. Virginia Mason Medical Center* (King County, WA 2019) (denying motion because there was no clear property at issue, the assertion of irreparable harm was insufficient, and monetary damages could compensate for any alleged harm). RJN Ex. 5. *Doe v. Partners Healthcare Systems Inc.* (Suffolk County, MA 2019) (denying motion without written reasoning). RJN Ex. 1. In *Doe v. Sutter Health* (Sacramento County, CA 2019) plaintiffs voluntarily dropped their Motion after the court granted Sutter Health's demurrer. RJN Ex. 3. Similarly, Plaintiffs' counsel sued Meta Platforms Inc., making claims about the use of Meta's cookie and tracking pixel technology on healthcare

B. PROCEDURAL BACKGROUND

Plaintiff Jane Doe brought an action against Google in *Jane Doe, et al. v. Google LLC*, 5:23-cv-02343 (N.D. Cal.) on May 12, 2023. Five days later, Plaintiffs John Doe I, et al., commenced this litigation, *John Doe I, et al. v. Google LLC*, 5:23-cv-02431 (N.D. Cal.). The Court consolidated the cases on June 30, 2023, and ordered Plaintiffs to file a consolidated complaint and preliminary injunction motion by July 13, 2023. The Court also ordered that Google's opposition to the motion should be combined with its motion to dismiss.

IV. LEGAL STANDARD

A. Preliminary Injunction

"[A] preliminary injunction is an extraordinary and drastic remedy, one that should not be granted unless the movant, *by a clear showing*, carries the burden of persuasion." *Doe v. Univ. of Wash.*, 695 F. App'x 265, 266 (9th Cir. 2017) (emphasis in original) (quoting *Mazurek v. Armstrong*, 520 U.S. 968, 972 (1997)). A party seeking a mandatory injunction—one that, as here, "goes beyond simply maintaining the status quo and orders the responsible party to take action"—faces a still higher burden. *Doe v. Snyder*, 28 F.4th 103, 111 (9th Cir. 2022). The Ninth Circuit has "cautioned" that such relief is "particularly disfavored." *Garcia v. Google Inc.,*, 786 F.3d 733, 740 (9th Cir. 2015). "In general, mandatory injunctions are not granted unless extreme or very serious damage will result and are not issued in doubtful cases." *Barrilleaux v. Mendocino County*, 2016 WL 4269328 at *2 (N.D. Cal Aug. 15, 2016) (quotations omitted). The "sliding scale" standard permitting preliminary injunctive relief where "a stronger showing of one element [...] offset[s] a weaker showing of another" (Mot. at 8) does not apply to mandatory injunctions. *See Snyder*, 28 F.4th at 111 n.4. Instead, the "court should deny such relief unless the facts and law clearly favor the moving party." *Garcia*, 786 F.3d at 740.

To obtain this drastic remedy, Plaintiffs must make a clear showing that: (1) they are likely

websites. *See In re Meta Pixel Healthcare Litig.*, 2022 WL 17869218 (N.D. Cal. Dec. 22, 2022). The allegations they made against Meta are distinct (for example, Meta does not offer pure analytics services), the technologies are different, and Google's defenses are different. Here, the data sent to GA is pseudonymous, Google prohibits the use of sensitive health information for advertising, and Google makes no attempt to re-identify anonymous users. Nevertheless, Judge Orrick denied a Preliminary Injunction as to Meta. *Id.*

to succeed on the merits of their claims; (2) they are likely to suffer irreparable harm absent a preliminary injunction; (3) the hardship they would suffer absent an injunction outweighs the hardship Defendants would suffer from entry of an injunction; and (4) an injunction is in the public interest (the "*Winter* factors"). *Winter,* 555 U.S. at 207.

B. Motion to Dismiss

Rule 12(b)(6) requires dismissal of a cause of action that fails to state a claim upon which relief can be granted. A plaintiff must plead factual allegations that "plausibly (not merely conceivably) entitle plaintiff to relief." *Maya v. Centex Corp.*, 658 F.3d 1060, 1067–68 (9th Cir. 2011). A claim is plausible only "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (requires more than a "sheer possibility," "naked assertion" or "formulaic recitation" of the elements of a cause of action). Nor must a court "'accept as true allegations that contradict matters properly subject to judicial notice or by exhibit.'" *Gonzalez v. Planned Parenthood of L.A.*, 759 F.3d 1112, 1115 (9th Cir. 2014) (citations omitted).

V. ARGUMENT

This District has repeatedly recognized that website and app developers have the right to employ analytics tools, and that the providers of those analytics tools, like Google, serve as mere vendors that provide companies with information about how users use their own websites and apps. *See, e.g.*, *Yale v. Clicktale, Inc.*, 2021 WL 1428400, at *3 (N.D. Cal. April 15, 2021) (dismissing privacy claims against defendant because it "is a vendor that provides a software service that allows its clients to monitor their website traffic."). Against this precedent, Plaintiffs' claims have no merit. Plaintiffs' motion for a preliminary injunction should be denied.

A. PLAINTIFFS SEEK A MANDATORY INJUNCTION

Plaintiffs seek a mandatory injunction, which is "subject to heightened scrutiny and should not be issued unless the facts and law clearly favor the moving party." *Barrilleaux v. Mendocino Cnty.*, 2016 WL 4269328 at *2 (N.D. Cal Aug. 15, 2016); *Garcia*, 786 F.3d at 740. "A mandatory injunction 'orders a responsible party to 'take action'" whereas, "[a] prohibitory injunction

prohibits a party from taking action and 'preserve[s] the status quo pending a determination of the action on the merits.'" *Marlyn Nutraceuticals, Inc. v. Mucos Pharma GmbH & Co*., 571 F.3d 873, 878–79 (9th Cir. 2009). Plaintiffs' requested relief does not seek to "preserve the status quo," which would entail Google maintaining its existing agreements with Health Care Providers. Rather, Plaintiffs ask the Court to do the opposite: to order Google to affirmatively identify a large number of websites and unilaterally terminate their GA, Ads, and Google Display contracts (without notice or an opportunity for these third-party providers to be heard). Mot. Notice at 2–3. Because this constitutes a mandatory injunction, Plaintiffs face a heightened burden to obtain the relief requested.

B. PLAINTIFFS FAIL TO MEET THE FOUR *WINTER* FACTORS

Plaintiffs' Motion fails because, (1) they are unlikely to succeed on the merits, (2) they are unlikely to suffer irreparable harm in the absence of preliminary relief, (3) the balance of equities favors Google, and (4) an injunction is not in the public interest. *Winter,* 555 U.S. at 207.

1. Plaintiffs Are Unlikely to Succeed on the Merits

Four of Plaintiffs' claims are at issue in the Motion: Violation of ECPA (Count 1); Violations of CIPA (Count 2); Intrusion upon seclusion (Count 4); and Violation of the UCL (Count 5). Each is likely to fail for at least one of five independent reasons: (1) Plaintiffs lack Article III Standing; (2) Google received no PII or PHI; (3) Plaintiffs consented to the Health Care Providers' use of cookies; (4) Google cannot be liable for merely serving as a vendor of analytics tools; and (5) Plaintiffs have failed to show that Google had the requisite knowledge or intent. Several claims fail for additional reasons outlined below.

a. Plaintiffs Lack Article III Standing

Plaintiffs are unlikely to succeed on the merits because they cannot establish Article III standing to seek injunctive relief. *See Timbisha Shoshone Tribe v. Kennedy,* 687 F. Supp. 2d 1171, 1187 (E.D. Cal. 2009) (holding serious standing issues preclude preliminary injunction). A plaintiff must establish standing for each form of relief sought. *Ellis v. Costco Wholesale Corp.*, 657 F.3d 970, 978 (9th Cir. 2011). To establish standing, the plaintiff must show evidence of: "(1) a concrete and particularized injury, that (2) is fairly traceable to the challenged conduct, and (3)

is likely to be redressed by a favorable decision." *Virginia House of Delegates v. Bethune-Hill*, 139 S. Ct. 1945, 1950 (2019). In addition to the standard Article III requirements, "a plaintiff seeking injunctive relief must additionally demonstrate a sufficient likelihood that he will again be wronged in a similar way." *Johnson v. JKLM Properties, L.L.C.*, 2020 WL 5517234, at *4 (N.D. Cal. Sept. 14, 2020). Plaintiffs cannot establish any of the elements of Article III standing.

First, Plaintiffs provide no evidence of an injury; they do not allege or show that Google used *their* information for any purpose other than to provide analytics services to the Websites. *See Hancock v. Urban Outfitters, Inc.* 830 F.3d 511, 514 (D.C. Cir. 2016) (sharing of alleged PHI "without any concrete consequence" does not give rise to an Article III injury). Plaintiffs do not show, for example, that Google used their health information to target ads to them. *Contra In re Meta Pixel Healthcare Litigation,* 2022 WL 17869218, at *3 (noting Smith received targeted advertisements after visiting the properties at issue in that action). Google does not allow PHI to be used in personalized advertising, and Plaintiffs provide no evidence to the contrary. Ganem Decl. Exs. 10, 12. And while a developer also has the option to link a GA account to their Google Ads account, Google still prevents the developer from targeting ads based on health conditions. Takabvirwa Decl. ¶¶ 6, 21; Zervas Decl. ¶¶ 49, 70.

Second, even had Google used the Websites' GA data transmitted for advertising or non-analytics related purposes, Plaintiffs provide no evidence to support their assertions that Google received any PII that could risk an injury-in-fact. *See Dinerstein v. Google, LLC*, 2023 WL 4446475, at *8 (7th Cir. July 11, 2023) (no standing where no allegation Google used anonymized medical records delivered to discern plaintiff's identity and Google explicitly agreed not to do so)*; Low v. LinkedIn Corp*., 2011 WL 5509848, at *3–4 (N.D. Cal. Nov. 11, 2011) (no standing where plaintiff was unable to articulate what personal information, aside from user identification number, had been transmitted to third parties, or how disclosure of ID could be linked to personal identity). The GA TOS prohibits third parties from sending Google PII and PHI, and Plaintiffs have not provided any evidence that any websites or apps violated these policies. Ganem Decl. ¶ 11 and Ex. 3; Zervas Decl. ¶¶ 62, 65. Google has further measures in place to prevent transmission of PII. Zervas Decl. ¶¶ 62–67; Ganem Decl. ¶¶ 31–50. In these circumstances, any alleged privacy injury

is unsupported by the record and too attenuated to support standing. *See Low*, 2011 WL 5509848, at *3–4; *Massie v. Gen. Motors LLC*, 2022 WL 534468, at *5 (D. Del. Feb. 17, 2022) (no standing to bring ECPA, CIPA, and invasion of privacy claims because "communications that do not involve personal information, [PII], or information over which a party has a reasonable expectation of privacy does not amount to a concrete injury"); *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 682 (N.D. Cal. 2021) (mere potential for privacy invasion based on an "attenuated chain of possibilities" insufficient for standing); *Dinerstein*, 2023 WL 4446475, at *8; *FTC v. Kochava, Inc.*, 2023 WL 3249809 (D. Idaho May 4, 2023) (consumers whose personal data is used for analytics but not tied to them "cannot be said to have suffered any privacy injury").

Third, even assuming Plaintiffs had suffered injury, they still would lack standing low because Plaintiffs' alleged injury is not "fairly traceable" to Google. *Virginia House of Delegates*, 139 S. Ct. 1945, 1950 (2019). Google—which does not enter into BAA agreements in connection with the relevant services—is not subject to HIPAA and is not responsible for any independent decisions made by the Websites to breach HIPAA and the GA TOS. *See Sneed v. Pan Am. Hosp.*, 370 F. Appx. 47, 50 (11th Cir. 2010) (HIPAA only "governs the use and disclosure of protected health information *by covered entities*") (emphasis added).

In any event, "because there is no private right of action under HIPAA, [Plaintiffs'] sole remedy for an alleged HIPAA violation is to lodge a written complaint with [the HHS]'". *Austin v. Atlina*, 2021 WL 6200679, at *3 (N.D. Cal. Dec. 22, 2021) (cleaned up). Here, Plaintiffs' requested relief is premised on an alleged HIPAA violation, as they define Health Information and Health Care Providers by reference to information and entities covered by HIPAA. Plaintiffs are improperly asking this Court to impose a remedy that only the HHS has the discretion to impose.

Finally, Plaintiffs cannot make the additional showing for injunctive relief that they will be wronged again in a similar way. Plaintiffs assert, under penalty of perjury, that they no longer use the Websites and will not use them in the future. Declaration of Jason Barnes ("Barnes Decl."), Exs. F–L, ¶¶ 9, 11. This mismatch between any alleged injury and the proposed remedy "poses a fatal [Article III] problem because granting preliminary relief would not redress the harm" Plaintiffs allege. *Overton v. Uber Techs., Inc.*, 2018 WL 1900157, at *2 (N.D. Cal. Apr. 20, 2018).

b. Plaintiffs' Consent Defeats All Claims

Plaintiffs consented to the Websites' use of cookies, which is fatal to each claim against Google. *See Matera v. Google Inc.*, 2016 WL 5339806, at *7 (N.D. Cal. Sept. 23, 2016) (CIPA); *Snipes v. Wilkie,* 2019 WL 1283936, at *6 (N.D. Cal. Mar. 20, 2019) (intrusion upon seclusion); *Calhoun v. Google LLC,* 526 F. Supp. 3d 605, 619 n.3 (N.D. Cal. 2017) (UCL). In order to use GA, Google required the Websites to expressly disclose their use of, and obtain consent to, the storing and accessing of cookies in connection with the use of GA, and they did just that. Ganem Decl. ¶ 11 and Ex. 4; Zervas Decl. ¶ 92. Many websites, including some at issue here, have large pop-ups inviting users to consent expressly to cookies. Zervas Decl. ¶ 93; *e.g.*, RJN Exs. 38–40. Google's Privacy Policy likewise discloses that Google may collect information about user interactions with third-party services that use Google's products. As Plaintiffs acknowledge, "Health Care Providers typically require acceptance of first-party cookies for a patient to engage with their web properties . . . ." CAC. ¶ 56. Because GA cookies are the Health Care Providers' first-party cookies—and because Plaintiffs understood they were consenting to such cookies—the Court should deny the injunction for this reason alone. Zervas Decl. ¶¶ 30, 39–41, 92.

Moreover, there is no basis for Plaintiffs' argument that any consent obtained is not valid because Google collected PHI. Mot. at 10–11. Plaintiffs provide no evidence that the Websites sent Google PHI in contravention of Google's restrictions. Ganem Decl. ¶ 11 and Ex. 3.

Finally, because each of Plaintiffs' claims is premised upon the collection of data from the Websites, and the Court may take judicial notice of the relevant terms of service and privacy policies of the Websites, the Court may also dismiss each and every claim under Rule 12(b)(6). *See, e.g.*, *Javier v. Assurance IQ, LLC*, 2021 WL 940319, at *2–3 (N.D. Cal. Mar. 9, 2021) (dismissing claims because plaintiffs consented to data collection described in privacy policy); RJN Exs. 21–37.

c. Plaintiffs' Wiretap Claim is Likely to Fail (Claim 1)

There are several other reasons Plaintiff's Wiretap claim is unlikely to succeed on the merits. First, Plaintiffs fail to state a Wiretap claim. Even if they had sufficiently pled a claim, the evidence demonstrates that (1) the Websites consented to GA, (2) Google is merely a vendor

and did not "intercept" any communications, and (3) Google's alleged conduct is not intentional.

i. Plaintiffs' Wiretap Claim Should Be Dismissed

Plaintiffs cannot show a likelihood of success on the merits because they have not adequately stated a claim. *See Sidiakina v. Bertoli*, 2011 WL 588289, at *2 (N.D. Cal. Feb. 10, 2011) (likelihood of success lacking where plaintiff failed to state a claim).

First, Plaintiffs' Wiretap claim fails because the consent of one party to the communication is a complete defense. 18 U.S.C. § 2511(2)(d); *Rodriguez*, 2021 WL 2026726, at *6. As the Websites chose to use GA, they obviously consented to it. *See* CAC ¶ 97.

Plaintiffs offer only the barest assertion that consent is invalid because it was acquired for a "criminal" or "tortious" purpose, "including but not limited to violation of the laws set forth [in the CAC]." CAC ¶ 211 n.79. Even had Plaintiffs alleged supporting facts, the "violations" set forth in the CAC stem from the same alleged interception, which is insufficient. *See Planned Parenthood v. Newman*, 51 F.4th 1125, 1136 (9th Cir. 2022) ("This criminal or tortious purpose must be separate and independent from the act of the recording."). Indeed, Google's policies demonstrate an utter lack of criminal purpose. Google explicitly prohibits developers from sending Google any PII or PHI, and Google has sophisticated technology to avoid linking data to individuals. *See supra* section V.B(1)(e).[7] In any event, Plaintiffs' theory that Google "encourages" the "interception" in order to profit from it is legally deficient. *Rodriguez*, 2021 WL 2026726 at *6 n.8 (holding Google's "purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money"); *Katz-Lacabe v. Oracle Am., Inc.*, 2023 WL 2838118, at

[7] Plaintiffs cite several cases their counsel have brought against health care providers for their deployment of third-party source code. In *Doe v. Virginia Mason*, the court denied the plaintiffs' preliminary injunction motion because plaintiffs did not allege irreparable harm and because the alleged information did not clearly constitute property. RJN Ex. 5. In *Doe v. Medstar*, the court dismissed plaintiffs' claims for violation of the Consumer Protection Act and breach of confidential relationship. As described in Section III.A.2, the court then denied plaintiffs' motion for class certification (noting that plaintiffs failed to show common issues predominate for three of their four claims, plaintiffs failed to show class certification was the superior method, and "[n]one of the class representatives read the complaint and all of them believed the Defendants had been guilty of intentionally or negligently leaking substantive confidential medical communications.") RJN Ex. 8 at 13. In *Doe v. Partners*, the court also denied plaintiffs' preliminary injunction motion. RJN Ex. 1.

*10 (N.D. Cal. Apr. 6, 2023).

Second, Plaintiff's Wiretap claim fails because a vendor who provides a tool for a website to record user interactions is not "intercepting" a communication and cannot be liable for the recording. *Graham v. Noom*, 533 F. Supp. 3d 823, 833 (N.D. Cal. 2021); *Williams v. What If Holdings, LLC*, 2022 WL 17869275, at *3 (N.D. Cal. Dec. 22, 2022).

Noom is directly on point. There, defendant Noom used the defendant FullStory's software to record "visitor data such as keystrokes, mouse clicks, and page scrolling," which allegedly resulted in the disclosure of "medical information" to FullStory without consent. *Noom*, 533 F. Supp. 3d at 823–29. The court held this could not violate CIPA because FullStory acted as a service provider to Noom, and the plaintiff did not plausibly allege that FullStory "aggregate[ed] [the] data for resale . . . [or that it] used the data itself." *Id*. Accordingly, at most, the defendant provided a "tool" that allowed Noom to "record and analyze its own data in aid of Noom's business." *Id*.[8]

Judge Alsup's reasoning in *Williams* also applies here: Google is effectively an independent third party hired to listen in on the Websites' communications and Google's software was merely a tool that the Websites used to record their own communications with plaintiffs. *Williams*, 2022 WL 17869275, at *3 ("[R]ecordation is routine documentation and therefore clerical in nature, which is qualitatively different from data mining."). That the vendor stores and processes the data on its own servers "is part of how the software tool functions" and does not by itself subject the vendor to liability. *Id.; see also Johnson v. Blue Nile, Inc*., 2021 WL 1312771, at *3 (N.D. Cal. Apr. 8, 2021) (holding same); *Yale v. Clicktale, Inc*., 2021 WL 1428400, at *3 (N.D. Cal. Apr. 15, 2021) (same).

Here, Google is alleged to be nothing more than a mere vendor to the Websites. It is developers who choose what content they wish to send Google, including whether anything constituting a "communication" is transmitted. *See, e.g.*, CAC ¶ 40, 97–99, 114, 130. The Websites

[8] "The analysis for a violation of CIPA is the same as that under the [ECPA]." *Hammerling v. Google LLC,* 615 F. Supp. 3d 1069, 1092 (N.D. Cal. 2022) (citation omitted). "Both statutes contain an exemption from liability for a person who is a 'party' to the communication, whether acting under the color of law or not." *In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d 589, 607 (9th Cir. 2020).

authorized Google—as their vendor—to receive the communications at issue and therefore Google could not have "intercepted" the alleged "communications" as a matter of law. Plaintiffs' Wiretap claim should therefore be dismissed.

ii. Plaintiffs Fail to Meet Their Evidentiary Burden

Even had Plaintiffs stated a claim, they fail to offer sufficient evidence to support a preliminary injunction.

a. The Websites' Consent Defeats the Wiretap Claim

To the extent that Plaintiffs argue they sufficiently alleged that the Websites did *not* consent to GA, that is easily refuted by the evidence. The Websites necessarily consented to GA by incorporating the Google code on their Websites and agreeing to the GA TOS. *See* Zervas Decl. ¶¶ 20, 39, 86; Ganem Decl. ¶ 11. That ends the inquiry.

b. Google Did Not "Intercept" Any Communication

The record is devoid of any evidence that Google used or processed information from the Websites contrary to their instructions. Google's role is limited to that of a service provider who created a tool "like a tape recorder" allowing the Websites "to record and analyze [their] own data in aid of [the Websites'] business." *Noom*, 533 F. Supp. 3d at 832–33. Indeed, there is no evidence that Google received sensitive health information from the Websites at all, nor that it used allegedly sensitive health information for advertising or any other purpose. While Plaintiffs' expert Smith opined in *In re Meta Pixel* that Facebook sent him health-related advertisements after visiting the Websites, Smith does not make that accusation here—nor do any of the Plaintiffs. *See In re Meta Pixel,* 2022 WL 17869218, at *3. Moreover, not only did Google not use sensitive health information for advertising, it would not have let the Websites use their own data for such purposes. Zervas Decl. ¶ 49. As in *Noom* and *Williams,* Plaintiffs' Wiretap claim fails.

c. Google's Lack of Intent is Fatal to the Wiretap Claim

Plaintiffs have not shown that Google "intentionally intercept[ed]" any communication. 18 U.S.C. § 2511. Plaintiffs make a single intent argument: that "Google has had specific knowledge of the problem" because Google forbids HIPAA-covered entities from sending Google PHI. Mot. at 6, 20. That argument lacks common sense. Plaintiffs cannot plausibly base such knowledge on

Google's policies *prohibiting* developers from sending Google the very information Plaintiffs claim to be the "problem." To the contrary, Google's policies clearly show that Google did not intend to receive any data that identifies users or reveals sensitive health information about them. And Google takes steps to prevent itself and its customers from using data from properties labeled Sensitive (such as healthcare provider properties) for targeted advertising. Google also refuses to enter into BAAs in connection with GA, evidencing an affirmative intent *not* to collect PHI. In addition, Google employs sophisticated technology to avoid linking data to individuals. *See supra* section III.A(3). Plaintiffs have not alleged, much less proved, any facts showing Google intended to receive personal health information in direct violation of its policies.

d. Plaintiffs' CIPA Claims are Likely to Fail (Count 2)

Plaintiffs' CIPA claims, which can only be brought by California resident John Doe II (*see infra* section V.D(2)), fail for similar reasons: (1) Google is merely a vendor and did not "intercept" or "record" any communications, and (2) Google's alleged conduct is not intentional.

i. Plaintiffs Fail to State a CIPA claim

Plaintiffs are unlikely to succeed on the merits because they do not plausibly state a CIPA claim. *See Sidiakina*, 2011 WL 588289, at *2. A claim under Penal Code section 631 requires showing that Google: (1) by means of any machine, instrument, or contrivance; (2) intentionally and without the consent of all parties; (3) read, attempted to read, or to learn the contents or meaning of any communication; (4) while the communication is in transit; (5) from or to any place within California. *See Adler v. Community.com, Inc.*, 2021 WL 4805435, at *3 (C.D. Cal. Aug. 2, 2021). A claim under section 632, requires showing: (1) Google intentionally listened to or recorded a communication; (2) using an electronic amplifying or recording device; (3) without the consent of all parties to the conversation; (4) where at least one of the parties intended the conversation to be confidential; and (5) that individual reasonably believed the communication would be confidential. CALCRIM No. 3010.

First, as explained above, as a mere vendor to the Websites, Google cannot be liable under Section 631 or 632 for "intercepting" a communication. *Noom*, 533 F. Suppp. 3d at 823; *Williams*, 2022 WL 17869275, at *3.

Second, Plaintiffs do not plausibly allege that Google purposefully and intentionally intercepted their PHI. The policies and restrictions Google implements, and the fact that the Health Care Providers control what they send to Google, undermine the naked assertions that Google intended to intercept Plaintiffs' PHI. *See* CAC ¶¶ 263–264, 435(e).

Third, CIPA applies by its own terms to communications "being sent from, or received at any place within this state." Cal. Penal Code § 631(a). Most of the Plaintiffs reside outside of California and allegedly interact with Health Care Providers equally outside of California. Even those Plaintiffs who currently reside in California fail to allege that they were within the state when they sent their communications. *See, e.g.*, CAC ¶¶ 20, 22, 29. Plaintiffs cannot support this element by merely alleging that Google is headquartered in California. *Hammerling v. Google LLC*, 2022 WL 17365255, at *10 (N.D. Cal. Dec. 1, 2022) (finding plaintiffs failed to allege interception in California despite allegation that Google is headquartered in California).

Fourth, section 632 does not apply where "the parties to the communication may reasonably expect that the communication may be overheard or recorded." Cal. Penal Code § 632(c). Because each of Plaintiffs' Health Care Providers disclosed their data collection and use, Plaintiffs' claim under section 632 must fail. RJN Exs. 21–37.

ii. Plaintiffs Fail to Meet Their Evidentiary Burden

Whether or not Plaintiffs stated a claim under CIPA, they offer no evidentiary support to warrant injunctive relief.

First, as stated above, Plaintiffs are unlikely to show that Google "intercepted" or "recorded" a "confidential communication." *See supra* section V.B(c)(i). Contrary to Plaintiffs' mischaracterization of basic facts, the alleged recording was performed by the Websites who deploy the Source Code, not Google. Zervas Decl. ¶¶ 20, 39, 86; Ganem Decl. ¶¶ 7–8; *see also* CAC ¶ 97. ***Second***, sections 631 and 632 require intentional conduct. Cal. Penal Code §§ 631(a) (prohibiting "intentional[] tap[ping]"), 632 (making liable a person who "intentionally and without the consent of all parties" records a confidential communication). As noted above, Plaintiffs do not and cannot establish intent and their CIPA claims are therefore bound to fail. *See supra* section V.B(c)(ii).

e. Plaintiffs' Privacy Claims are Likely to Fail (Count 4)[9]

California's common law intrusion-upon-seclusion claim requires a plaintiff to plead that (1) "the defendant [] intentionally intrude[d] into a place, conversation, or matter, as to which the plaintiff has a reasonable expectation of privacy," and (2) "the intrusion [] occur[ed] in a manner highly offensive to a reasonable person." *Hernandez v. Hillsides, Inc*., 47 Cal. 4th 272, 286 (2009). The common law "set[s] a high bar for an invasion of privacy claim." *Belluomini v. Citigroup, Inc.*, 2013 WL 3855589, at *6 (N.D. Cal. July 24, 2013). This claim is likely to fail for five reasons: (1) Plaintiffs have not stated a plausible claim; (2) Google is not an unauthorized third party; (3) Google did not have the requisite intent; (4) Plaintiffs do not have a recognized privacy interest in the data transmitted, which was not identifiable and did not contain PII or PHI; and (5) there is no highly invasive intrusion. It is further likely to fail because the CAC fails to state a plausible claim.

i. Plaintiffs' Privacy Claims Should be Dismissed

Plaintiffs plead insufficient facts to state a plausible claim for invasion of privacy.

First, setting aside Plaintiffs' bare assertions of intent, their allegations regarding Google's policies against the collection they allege, and the fact that providers control what data is transmitted, negate their claims that Google "intended" to violate their privacy. *See Caraccioli*, 167 F. Supp. 3d at 1063. Nor do Plaintiffs plausibly allege a reasonable expectation of privacy because the alleged tracking was disclosed and consented to. *Heldt v. Guardian Life Ins. Co. of Am.*, 2019 WL 651503, at *6 (S.D. Cal. Feb. 15, 2019) (finding no reasonable expectation of privacy in plaintiff's medical information when plaintiff consented to disclosure).

Second, Plaintiffs cannot establish a "serious intrusion" into their reasonable expectation of privacy because they offer only conclusory assertions of what Google allegedly obtained. *See Kurowski v. Rush Sys. for Health*, 2023 WL 4707184, at *3 (N.D. Ill. July 24, 2023) (dismissing claims where plaintiffs did not allege what specific data was collected). Each Plaintiff offers an identical, generalized statement that they exchanged "communications" with providers, including

[9] The elements for invasion of privacy under the California Constitution (Claim 3) and for the common law claim of intrusion upon seclusion (Claim 4) are sufficiently similar that courts consider them together. *In re Facebook*, 956 F.3d at 601. The analysis here thus applies equally to both claims.

"conditions, treatments, providers, and appointments." CAC ¶¶ 19–31. Plaintiffs allege only generalized and undifferentiated conduct untethered to any particular Plaintiff's experience. These conclusory statements are insufficient. *Cousin v. Sharp Healthcare*, 2023 WL 4484441, at *3 (S.D. Cal. July 12, 2023) (conclusory assertions of disclosure of "sensitive medical information; communications and messages with doctors; medical test results; payment information" and other data insufficient to support a claim); *see also Hammerling*, 2022 WL 17365255, at *8–9 (while allegations that Google collected information based on a list of apps visited and products plaintiff viewed was "more specific" than allegations about information "Google may have gleaned from [the plaintiffs'] use of . . . third-party apps," the more specific data was "still not sufficiently personal, nor its collection sufficiently harmful, to be highly offensive"). Plaintiffs' allegations are far too vague to allow this Court to conclude that Google intercepted personal information, let alone that the intrusion was serious. Plaintiffs fail to state a common law or constitutional privacy claim.[10]

ii. Plaintiffs Fail to Meet Their Evidentiary Burden

Plaintiffs also fall short of their burden of providing evidence to support their deficient allegations. ***First,*** Plaintiffs base their intrusion claim upon Google being an unauthorized "third party" to the purported communication. *See, e.g.,* CAC ¶ 362. But because Google is an authorized recipient of the communication (as a vendor to the Websites), it could not have engaged in an intrusion at all. *See supra* section V.B(c)(i); *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 830 (N.D. Cal. 2020) (dismissing intrusion upon seclusion claim where Plaintiffs failed to state ECPA claim and CIPA claim).

***Second*,** failure to plausibly demonstrate intent is fatal to the claim. *Caraccioli v. Facebook, Inc.*, 167 F. Supp. 3d 1056, 1063 (N.D. Cal. 2016) ("intrusion upon seclusion . . . require[s] intent on the part of the tortfeasor" and plaintiff failed to plead Facebook's intent where "the allegations

[10] In addition, the California Constitution does not apply extraterritorially and cannot be applied to out-of-state Plaintiffs. *See People ex rel. DuFauchard v. U.S. Fin. Mgmt., Inc.*, 169 Cal. App. 4th 1502, 1516 (2009) (statutes are presumed not to apply extraterritorially); *People v. Bustamante*, 57 Cal. App. 4th 693, 699 n.5 (1997) (constitutional provisions and statutes construed the same way).

in the amended complaint contradict the incorporated Terms of Service"). As stated above, Plaintiffs have not shown the requisite intent. *See supra* section V.B(c)(ii).

Third, since there is no evidence that Google received any PII or PHI from the Websites, there is no reasonable expectation of privacy in the data transmitted to Google. *See London v. New Albertson's, Inc.*, 2008 WL 4492642, at *8 (S.D. Cal. Sept. 30, 2008) (no protected privacy interest in de-identified medical information); *Cousin*, 2023 WL 4484441, at *3–4 ("While Plaintiffs provide an example of a search by a hypothetical patient, they fail to state what information they each provided to [Sharp] . . . that was subsequently disclosed to Meta."). Plaintiffs are left with a complaint that Google legally provided the Websites with analytics services, as contracted by the Websites, relating to pseudonymized information.

While certain courts have held that cookies or URLs could be considered PII in certain situations, that is dependent on the URLs being linked to an identifiable person, and cookies being collected after a user has signed out. *See Facebook Tracking*, 956 F.3d at 603–04, (distinguishing cases involving URLs alleged to be correlated with user ID).

Here, Google prevents PII from being connected with pseudonymous identifiers absent user consent, and takes steps to separate pseudonymized data from users' identities. Zervas Decl. ¶ 67, 80–82; Ganem Decl. ¶¶ 31–50. Even if Client ID, AdID, or IDFA could be considered PII, that is only to the extent that they are linked with an identifiable person, and they never are. A Google user may, however, themselves choose to save their browsing history and app activity in their Google Account (associated to their account but not to a pseudonymous identifier) by enabling WAA, sWAA (disabled by default), GAP, and NAC (disabled by default), and even then, only if the relevant developers affirmatively enable Signals. Ganem Decl. ¶ 41. Plaintiffs provide no evidence that these circumstances are present here, and even if they were, such information still would not be used for ads personalization. *See* Takabvirwa Decl. ¶¶ 29–31. Thus, Dr. Shafiq's evidence regarding how Google *can* use multiple types of data to identify individuals is irrelevant. There is no evidence that Google does so other than with user consent, and even then, still not for personalization of advertising. Zervas Decl. ¶¶ 80–84, 146.

This Court has held that browser settings and the contents of cookies from pages containing

publicly available medical information does not relate specifically to the user's health. *See Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 954–55 (N.D. Cal. May 9, 2017) (finding that neither "browser settings, language, operating system, IP address, and the contents of cookies" nor the URLs for pages "containing information about treatment options for melanoma, information about a specific doctor, [or] search results related to the phrase 'intestine transplant'" constitute PHI); *Cousin*, 2023 WL 4484441, at *3 (information about plaintiffs' use of a public website to 'research ... doctors,' 'look for providers,' and 'search for medical specialists' was not considered PHI because 'nothing about [the] information relates specifically to Plaintiffs' health'"). In fact, in another parallel lawsuit brought by Plaintiffs' counsel against a Health Care Provider, the court found that the information allegedly collected "does not in the least bit fit into" the category of health information covered by HIPAA. *Kurowski*, 2023 WL 4707184, at *4.

Finally, even if Plaintiffs had a privacy interest in the data allegedly received by Google (they do not), any alleged intrusion is not highly invasive. Contrary to Plaintiffs' allegation, Google does not place code on Health Care Provider properties. Zervas Decl. ¶¶ 20, 39, 86; Ganem Decl. ¶¶ 7–8. Additionally, Google vigorously avoids receiving PHI: it prohibits developers from transmitting PHI, it refuses to enter into BAAs, and it ensures that no data from healthcare provider websites and apps are used for targeted advertising. Ganem Decl. ¶¶ 11, 15, 16; Takabvirwa Decl. ¶ 6. Even if a HIPAA Covered Entity mistakenly sends Google PHI in contravention of HIPAA and Google's policies, that cannot constitute a highly invasive intrusion *by Google*. HHS, which is tasked with enforcing HIPAA, has not prohibited the use of analytics technology, and has recently reminded HIPAA-regulated entities that *they* "are required to comply with the HIPAA Rules *when* using tracking technologies." RJN Ex. 42 (emphasis added). Further, Plaintiffs do not provide any evidence showing that Google used any information they provided to the Websites for purposes other than providing the Websites with analytics services. Plaintiffs have not provided evidence of any actionable privacy violation, much less a highly invasive one.

f. Plaintiffs' UCL Claim is Likely to Fail for Lack of Standing (Count 5)

Plaintiffs' UCL claim will also fail because (1) they have failed to demonstrate UCL

standing, and (2) they have not supported a viable UCL claim. Not only does Plaintiffs' lack of standing doom their request for an injunction, it compels dismissal of their claim.

"[T]he UCL limits standing to those who have 'suffered injury in fact and lost money or property as a result of . . . unfair competition." *Rodriguez*, 2021 WL 2026726, at *8 (citation omitted). "[C]ourts have widely held that 'personal information' does not constitute money or property under the UCL." *Gardiner v. Walmart, Inc*., 2021 WL 2520103, at *8 (N.D. Cal. Mar. 5, 2021); *Oracle*, 2023 WL 2838118, at *8 (dismissing UCL claim for lack of standing because "the 'mere misappropriation of personal information' does not establish compensable damages"); *Rodriguez*, 2021 WL 2026726, at *8 ("[N]o federal court has wedged individual digital data into the UCL's 'money or property' box"); *Gonzalez v. Uber Techs., Inc*., 305 F. Supp. 3d 1078, 1093 (N.D. Cal. 2018) ("[T]he sharing of names, user IDs, location and other personal information does not constitute lost money or property for UCL standing purposes.").

Plaintiffs' allegations that Google may benefit from their data does not cure the deficiency. Mot. 18; CAC. ¶¶ 267–293; *see, e.g.*, *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1040 (N.D. Cal. 2019) ("That the information has external value, but no economic value to plaintiff, cannot serve to establish that plaintiff has personally lost money or property."). Nor do Plaintiffs allege that they suffered economic injury as a result of reliance on any misrepresentations *Google* made, nor that they paid to use the Websites. In any event, for Plaintiffs' harm to be "fairly traceable" to Google's alleged misrepresentations under the UCL, "Plaintiffs must have seen the misrepresentations and taken some action based on what they saw." *In re iPhone Application Litig.*, 6 F. Supp. 3d 1004, 1015 (N.D. Cal. 2013) (finding no UCL standing where Plaintiffs failed to establish actual reliance on Apple's alleged misrepresentations). Here, Plaintiffs do not provide evidence (or even allege) that they read these policies (or any other Google representation) in connection with their use of the Websites. CAC. ¶ 383; *see Rodriguez*, 2021 WL 2026726, at *8 (no UCL standing where plaintiffs did not contend that any transactions were taken "because of [their] understanding of the [App's] data practices vis-a-vis Google.").[11]

[11] The court in *Calhoun* held that allegations of the loss of personal information sufficiently stated an "economic injury" under the UCL. *Calhoun*, 526 F. Supp. 3d at 636. But courts have

Finally, the UCL claim has no likelihood of success because Plaintiffs cannot show, as they allege in conclusory fashion, that "Google assures users of all Google products that it will not collect Health Information without users' consent but in reality *knows* (or should have known) that the Google Source Code and advertising products are being improperly used on Health Care Provider web properties." CAC. ¶ 378 (emphasis added). As set out above, Plaintiffs cannot show this is the case. *See supra* section V.B(c)(ii). And any such theory is subject to Rule 9(b)'s heightened pleading standards. At bottom, Plaintiffs cannot show that Google acted unlawfully, unfairly, or fraudulently where Google acted only in its authorized and disclosed capacity as an analytics provider for the Websites.

2. Plaintiffs Have Not Established Harm, Much Less Irreparable Harm

This motion should also be denied because Plaintiffs cannot show irreparable harm. *See Winter,* 555 U.S. at 375. Speculative injury is not sufficient, and there must be more than an unfounded fear; a preliminary injunction is not simply to prevent the possibility of some remote future injury. *GEC US 1 LLC v. Frontier Renewables, LLC*, 2016 WL 3345456, at *5 (N.D. Cal. June 16, 2016). Plaintiffs fail to show irreparable harm for three reasons.

First, Plaintiffs are not likely to suffer *any* harm. Plaintiffs failed to provide any evidence to show any past injury, and they have stopped using the Websites. *Overton*, 2018 WL 1900157, at *2; *see supra* section V.B.1(a).

Second, Plaintiffs' irreparable harm argument is purely speculative. *See GEC US 1 LLC*, 2016 WL 3345456, at *5; *Lockheed Missile & Space Co. v. Hughes Aircraft Co*., 887 F. Supp. 1320, 1325 (N.D. Cal. 1995). Plaintiffs allege only that Google is "capable" of linking data without users' consent and using it for targeted ads, but submit no evidence that Google actually does so.

---

subsequently rejected this holding as erroneous. As explained by another judge in this District, *Calhoun* relied on cases addressing Article III standing, which is distinct. *See, e.g., Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461, 484 n.8 (N.D. Cal. 2021) ("This court disagrees with the holding in *Calhoun*."). And as another judge in this District explained, the UCL case *Calhoun* cited for its holding rejected the conclusion that *Calhoun* reached. *Wesch v. Yodlee, Inc.*, 2021 WL 6206644, at *4 (N.D. Cal. July 19, 2021) ("Additionally, *Calhoun* cites *In re Facebook Privacy Litigation* as support for standing under the UCL, but the Ninth Circuit explicitly rejected this theory in that case."); *see also Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1145 (E.D. Cal. 2021).

See CAC. ¶¶ 168, 170, 175–79. *See Dinerstein*, 2023 WL 4446475, at *7 (finding threat of harm speculative where data use agreements prohibited Google from using medical information to identify an individual). Here, Google is not linking data, selling Plaintiffs' information, using data from the Websites to personalize advertising, or disclosing Plaintiffs' information to anyone.

In any event, Plaintiffs' requested relief is unnecessary. Google prohibits Covered Entities from transmitting PHI and PII, and Plaintiffs have not provided any evidence to show that any Health Care Provider is violating Google's prohibitions. Zervas Decl. ¶¶ 62–66. In addition, Google ensures that no data from Health Care Providers is used for targeted advertising. Takabvirwa Decl. ¶ 6. Finally, Google prohibits any website or app from using sensitive data, including information about health conditions, in targeted advertising, and has a robust ad review process that can result in the suspension of a Google Ads account if any violation is discovered. *Id.* ¶¶ 21-23. Additionally, both Alton Memorial and Medstar no longer use Google services in authenticated pages, further making part of the requested relief moot, as Plaintiffs' counsel acknowledged in their action against *Medstar*. *See* Smith Decl. ¶ 154; RJN Exs. 10, 11.

3. The Balance of Equities Disfavors an Injunction

"An injunction may not issue unless the balance of hardships tips sharply in favor of the moving party." *Disney Enters. v. VidAngel, Inc*., 224 F. Supp. 3d 957, 977 (C.D. Cal. 2016). The balance of hardships favors Google because enjoining it from "acquir[ing]" and "using" so-called Health Information from Health Care Providers would be excessively burdensome and/or infeasible. Plaintiffs allege Google's conduct affects individuals who visit more than 2,989 Healthcare Provider properties. Mot. Notice at 2. Disabling those websites' accounts is one thing, but identifying which of the other millions of developers that use GA fall within Plaintiff's definition of "Health Care Providers" can only be done manually, because Google does not classify domains by whether they are health care providers. And while Google does classify health-related websites for sensitivity classifications, that includes far more than just health care providers as Plaintiffs define it, including websites that have nothing to do with this case.[12]

[12] In support of this ambitious request, Plaintiffs rely on verticals, previously used by a deprecated Google product (AdWords Application Programming Interface) entirely separate

4. An Injunction is Not in the Public Interest

The public interest also disfavors an injunction because both Health Care Providers and users of their websites benefit from the use of GA, Ads, and Display. GA is a freely available product that providers need to make informed decisions about and improve their websites, which would otherwise require expensive in-house design and technical expertise. Teehan Decl. ¶ 18. The use of products like GA helps make healthcare cost-efficient and accessible, ultimately benefiting both the healthcare providers and the users of their websites. *Id*. ¶¶ 31-32. For example, the American Hospital Association has stated that providers rely on analytics to provide the public with important health information. *Id*. Ex. 1 (AHA Letter). Additionally, the use of Google Ads and Display allow Health Care Providers to market their companies and similarly provide the public with important health information and make healthcare cost-efficient. Ordering Google to unilaterally terminate its GA, Google Ads, and Display agreements with all Health Care Providers without any basis to believe they are violating Google's policies is not in the public interest.

Other than alleging a vague public interest in protecting one's right to privacy, Plaintiffs provide no basis for why a preliminary injunction would serve the public interest. Mot. 21–22. The HHS, which represents the public interest and is tasked with enforcing HIPAA, recently issued a bulletin discussing analytics technology. RJN Exs. 41, 42. Rather than prohibiting the use of analytics technology altogether, as Plaintiffs would have this Court do, the HHS only reminded HIPAA-regulated entities that they "are required to comply with the HIPAA Rules *when* using tracking technologies."[13] *Id.* Ex. 42 (emphasis added). Disallowing all healthcare provider websites from improving those websites by using a technology service used by millions of other developers would not serve the public interest. This Court should decline to accept Plaintiffs' unsubstantiated and overreaching proposition—one that the HHS notably declined to reach—that the use of GA by all healthcare providers automatically constitutes a privacy breach.

---

from GA. GA does not maintain a list of "health care provider" properties and does not know which, if any, developers deploy GA code on health care provider properties. Ganem Decl. ¶ 51. *See also* Zervas Decl. ¶¶ 77–78, 137, 148.

[13] Notably, the court in *Kurowski* found this bulletin warranted no deference because "its guidance goes well beyond what [HIPAA] can bear." 2023 WL 4707184, at *4.

C. AN INJUNCTION COULD NOT BE DEFINED WITH PARTICULARITY

Rule 65(d)(1) requires that an injunction describe in "reasonable detail" what is to be restrained. This rule requires the language of injunctions to be reasonably clear so that ordinary persons will know precisely what action is proscribed. *United States v. Holtzman*, 762 F.2d 720, 726 (9th Cir. 1985); *Lamont v. Krane*, 2019 WL 2010705, at *3–4 (N.D. Cal. May 7, 2019) (declining to issue injunction where it could not be described with particularity).

Here, Plaintiffs allege that at least 2,989 unidentified Health Care Provider properties "redirect[] patient Health Information to Google Analytics." CAC ¶ 47. While the parties can quibble over which of those properties are actually covered by HIPAA and engaging in the challenged conduct, Google has no realistic way of categorically determining which of the millions of other developers that use GA are "Health Care Provider properties" as Plaintiffs define them, nor which developers engage in the specific conduct Plaintiffs complain of. Ganem Decl. ¶ 51. The categorizations Google does use (for example, for ads sensitivity classifications) are both under and over inclusive. Zervas Decl. ¶¶ 77–78, 137, 147.

D. PROVISIONAL CLASS CERTIFICATION SHOULD BE DENIED

Provisional class certification should be denied because class certification is unnecessary for the preliminary injunction requested by Plaintiffs and Plaintiffs cannot demonstrate that their proposed provisional class satisfies the requirements of Rules 23(a) and 23(b)(2).

1. Class Certification is Unnecessary for the Proposed Injunctive Relief

"In the absence of class certification, a preliminary injunction may be issued only for the named [Plaintiffs]." *Roman v. Wolf*, 2020 WL 3869729, at *1 (C.D. Cal. Apr. 23, 2020) (citing *Nat'l Ctr. for Immigrants Rights, Inc. v. INS*, 743 F.2d 1365, 1371 (9th Cir.1984)). Here, Plaintiffs request that Google be enjoined from acquiring all Health Information from an enumerated list of Health Care Providers, each of which Plaintiffs allege to have used (but do not plan to use again). Since GA cannot be used by a given website for only certain users and not others, if the proposed preliminary injunction is granted with respect to the named Plaintiffs, it will have the effect of prohibiting the use of GA for all users of the Websites. Class certification is therefore unnecessary and the Court need not reach the merits of it.

2. Plaintiffs Cannot Satisfy Rule 23(a)'s Commonality Requirement

In any event, provisional class certification should be denied because Plaintiffs cannot establish common legal or factual issues. Whether the challenged conduct occurred as to any specific class member depends on a host of individualized, user- and Website-specific inquiries:

- **Consent**: While the Court could evaluate the disclosures and consents obtained by the Websites named in the Complaint, it could not feasibly evaluate the disclosures of the approximately 3,000 websites Plaintiffs generically reference. The question of consent, which is common to all of Plaintiffs' claims, cannot be answered on a class-wide basis because each website's disclosures will need to be considered by this Court. *See* Mot. at 8 ("consent is a common defense for each claim"); *Quesada v. Banc of Am. Inv. Servs., Inc.*, 2013 WL 623288 (N.D. Cal. Feb. 19, 2013) (denying class certification where plaintiffs did not propose a realistic means for classwide resolution of consent).

- **Communications**: The proposed class includes not only patients who log into patient portal accounts, but also users who do not have patient portal accounts and who visit Health Care Providers' publicly accessible websites for information only. The inquiry into whether users' activity constitutes a "confidential" communication is necessarily varied. *See Cousin*, 2023 WL 4484441, at *3 (Even within a given Website, the information any given user entered will differ. Users may visit a Website for any number of reasons, e.g., to check operating hours, get directions, or look for a job).

- **Use of GA by Websites**: each Website differs in how it uses and what information it shares with GA. For example, Websites will have different URLs, and will differ in whether they use Custom Events, and if so, which ones.

Plaintiffs' focus on the reductive question of "how the Google Source Code operates" elides these problems. Cutting off a valuable product to broad swaths of the Internet and its users on a classwide basis is improper. How the Source Code operates depends on the highly individual practices and settings of each one of the 2,989 websites and innumerable class members.

Additionally, because the law of multiple jurisdictions would apply to a nationwide class, variances in state law overwhelm common issues. *See Zinser v. Accufix Rsch. Inst., Inc.*, 253 F.3d 1180, 1189–90 (9th Cir. 2001). Plaintiffs contend that California law should apply across the board because of the choice of law clause in Google's TOS. But the TOS concerns *Plaintiffs'* use of Google's services—not Plaintiffs' use of third-party websites that may use Google's services,[14]

[14] Google's TOS list the services that they govern. None of the services at issue here are listed. *See https://policies.google.com/terms/service-specific?hl=en-US.*

and which may select other state laws to govern disputes.[15]

Even if the choice of law clause facially applies to Plaintiffs' use of third-party services, California law still requires consideration of whether enforcement of that provision is appropriate, which considers the various states' interests in the dispute. *Bridge Fund Cap. Corp. v. Fastbucks Franchise Corp*., 622 F.3d 996, 1002 (9th Cir. 2010) (identifying considerations governing enforceability of choice of law clauses). Here, critical differences between the laws of California and those of the states where some of the named Plaintiffs reside confirm that Plaintiffs may not invoke California law on behalf of non-California residents—both named Plaintiffs and class members that reside outside of California. *See In re Yahoo Mail Litig*., 308 F.R.D. 577, 602 (N.D. Cal. 2015) (holding class members' claims should be governed by wiretapping laws of each state); *Hammerling*,, 2022 WL 17365255, at *11 (CIPA does not apply outside California); *United States v. Luong*, 471 F.3d 1107, 1109 (9th Cir. 2006) (holding interception occurs "where the tapped phone is located and where the [alleged eavesdropper] first overhear[s] the call."); *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 129–31 (3d Cir. 2022) (reasoning from *Luong* and other decisions that electronic communications are intercepted on plaintiffs' browsers—i.e., where the cookies sit and reroute data).

Additionally, the differences between the intrusion laws between California and, for example, Illinois, where Jane Doe II resides, are "not trivial" as each state "may impose or not impose liability depending on" its own policy choices." *Mazza,* 666 F.3d at 591.

2. Plaintiffs Cannot Satisfy Rule 23(b)(2)

Plaintiffs also fail to satisfy Rule 23(b)(2), which "applies only when a single injunction or declaratory judgment would provide relief to each member of the class." *Dukes*, 564 U.S. at 360. Class certification under Rule 23(a) and (b)(2) requires two steps: (1) the identification of a common legal problem, and (2) a showing that the common legal issue may be resolved as to all class members simply by virtue of their membership in the class. *Id.* at 360.

[15] Pursuant to some of the Websites' choice of law provisions, at least four other state laws apply to the disputes between some of the Websites and their users. *See* RJN Ex. 24 (Maryland); RJN Ex. 31 (Missouri); RJN Ex. 30 (Minnesota); RJN Ex. 26 (Illinois).

First, Plaintiffs cannot pursue injunctive relief because they no longer use the Websites and do not intend to do so again. Barnes Decl., Exs. F–L, ¶¶ 9, 11. Plaintiffs are thus not a member of any class entitled to injunctive relief. *See Lucas v. Breg, Inc.*, 212 F. Supp. 3d 950, 972 (S.D. Cal. 2016) (denying certification as to a (b)(2) class because the named plaintiffs did not intend to use the product again).

Second, many putative class members may object to the proposed injunction if they believe they benefit from the use of GA on websites to improve accessibility and availability of healthcare. *See D.B. ex rel. Doe 1 v. Brooks-Lasure*, 2022 WL 16840325, at *12 (N.D. Cal. Nov. 9, 2022) (denying certification where class members may not want plaintiffs' requested relief).

Plaintiffs have thus not shown that the requested injunctive relief would be appropriate for all class members or would "redress [Plaintiffs'] alleged injuries or those of the class [they] seek[] to represent." *Murray v. Sears, Roebuck & Co*., 2014 WL 563264, at *10 (N.D. Cal. Feb. 12, 2014). The same reason precludes a finding of adequacy under Rule 23(a). *See e.g. Alberghetti v. Corbis Corp.,* 263 F.R.D. 571, 577–78 (C.D. Cal. 2010) ("[A] class representative is not adequate if the representative seeks relief which the class members do not want.").

Plaintiffs have failed to meet their burden under Rule 23, and provisional class certification is unnecessary. The Court should deny provisional class certification.

VI. MOTION TO DISMISS

Plaintiffs' complaint illustrates that 150 pages of meandering allegations can still fail to meet Rule 8's requirement of a "short and plain statement of the claim showing that the pleader is entitled to relief," let alone the heightened specificity Rule 9(b) requires here.[16]

A. The Heightened Standard of Rule 9(b) Applies

Rule 9(b) requires plaintiffs to plead the circumstances constituting fraud with particularity. It applies wherever a plaintiff asserts fraudulent conduct, whether or not the plaintiffs' claim is styled as fraud. *See Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1124 (9th Cir. 2009); *Apumac, LLC v. Flint Hills Int'l*, 2015 WL 13306128, at *5 (C.D. Cal. Feb. 6, 2015)

[16] This section discusses only those claims not addressed in Plaintiffs' motion for a preliminary injunction, which should be dismissed for the reasons discussed above.

(noting that "Rule 9(b) applies to allegations of fraud, not just claims of fraud"); *see also Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1103 (9th Cir. 2003). Plaintiffs allege that Google collected their information by "disguising" its "secretly embedded" Source Code as first-party cookies. CAC ¶¶ 4, 56, 59(c), 249. Plaintiffs allege this collection occurs even though Google promises to the world that it won't do it. *See, e.g.*, CAC ¶ 250. Plaintiffs further allege that even as it makes certain promises to users, Google conspires with advertisers to break these promises. CAC ¶¶ 251–62. This sounds in fraud, rendering Plaintiffs claims subject to Rule 9(b). *See Rodriguez*, 2021 WL 2026726, at *6 (where plaintiffs alleged a "sensational" plot about how Google Analytics works, Rule 9(b) demanded dismissal because plaintiffs failed to allege "when the 'secret scripts' plot was hatched; which Google departments (let alone employees) were involved; and anything resembling a particular date, time, or place"); *Hidden Empire Holding, LLC v. Angelone*, 2023 WL 4208067, at *17 (C.D. Cal. May 10, 2023) (noting claims involving promises without intention to honor the promise sounded in promissory fraud).

B. Trespass to Chattels (Count 6)

"Trespass to chattels lies where an intentional interference with the possession of personal property has caused injury." *Best Carpet Values, Inc. v. Google LLC*, 2021 WL 4355337, at *4 (N.D. Cal. Sept. 24, 2021) (citing *Intel Corp. v. Hamidi*, 30 Cal. 4th 1348, 1350–51 (2003)). Where, as here, the trespass concerns "unauthorized electronic contact with computer systems," the plaintiff must establish that the contact damaged the computer system or impaired its functioning. *Intel*, 30 Cal. 4th at 1352. Aside from conclusory assertions, Plaintiffs fail to allege facts sufficient to support any element of this claim.

1. Plaintiffs Fail to Allege Intent

A trespass claim requires the defendant's *intentional* interference with the plaintiff's personal property. *Best Carpet*, 2021 WL 4355337, at *4. Although Plaintiffs offer the bare assertion that Google intentionally placed cookies on the Plaintiffs' devices, Plaintiffs' factual allegations establish the opposite. Indeed, Plaintiffs illustrate that it is the "Health Care Provider" that "deployed the Google Source Code" and "had Google Cookies lodged on [the Plaintiffs'] computing device[s]." CAC ¶ 398; *see also id.* ¶ 40 ("Google Source Code is

provided by Google in a copy-and-paste format . . . .").

2. No Interference with Plaintiffs Personal Property

The tort of trespass protects *possessory* interests in property. *Intel*, 30 Cal. 4th at 1359. Yet Plaintiffs' complaint centers on data that was never in Plaintiffs' possession.

Plaintiffs allege that the data at issue concerns Plaintiffs' activities on third-party websites. (*See, e.g.*, CAC ¶¶ 36, 52–64). This information would not exist but for the intervention of the software the Websites deployed. Since it is the Health Care Providers that create the data and control whether and to what extent others may access it, it is the Health Care Providers that possess the data—not Plaintiffs. *See Alderson v. United States*, 718 F. Supp. 2d 1186, 1197 (C.D. Cal. 2010) ("With respect to Plaintiffs' apparent argument that information *qua* information is 'property,' this argument fails. In order to possess a property right, whether tangible or intangible, a person must be able to exclude others from using or taking the purported property.").

Indeed, California courts have held that allegedly unauthorized copying of electronic information, without more, fails to implicate a cognizable property interest. *See Casillas v. Berkshire Hathaway Homestate Ins.*, 79 Cal. App. 5th 755, 764–65 (2022) (rejecting trespass claim based on copying of files and collecting authorities); *Intel*, 30 Cal. 4th at 1361–62 ("[T]he appropriate tort is not trespass.").

3. Plaintiffs Fail to Plausibly Allege Actual Loss

Plaintiffs do not and cannot plausibly allege damage to or loss of function of their devices. *Intel*, 30 Cal. 4th at 1147. California state and federal courts routinely hold that the placement of cookies or the interception or copying of personal data is insufficient to support the "actual loss" requirement of a trespass claim. *See, e.g.*, *Casillas*, 79 Cal. App. 5th at 764; *WhatsApp Inc. v. NSA Grp. Technologies Ltd.*, 472 F. Supp. 3d 649, 685–86 (N.D. Cal. 2020) (dismissing trespass claim based on the installation of malware on plaintiff's servers that diverted communications to defendants); *LaCourt v. Specific Media, Inc.*, 2011 WL 1661532, at *7 (C.D. Cal. Apr. 28, 2011) (defendant's alleged placement of tracking cookies for targeted advertisement did not result in the impairment required to state a claim for trespass).

Plaintiffs offer the naked assertion that the alleged trespass caused the "total deprivation of Plaintiffs' and Class Members' use of their computing devices to communicate with Health Care Providers," (CAC ¶ 404(d)), but this unsupported assertion makes no sense and was correctly rejected in a parallel case brought by Plaintiffs' counsel against a Health Care Provider. In *Kurowski*, the court found that the plaintiffs could not plausibly establish that the placement of cookies degrades the functionality of the plaintiffs' devices where, as here, the plaintiffs had alleged that the Health Care Provider's "placement of cookies was so invisible and surreptitious that she was completely unaware of it." 2023 WL 4707184, at *10. Further, common sense dictates that Google cannot "intercept" any communications if Plaintiffs are unable to use their devices for communicating with providers. Far from rendering the devices inoperable, the allegations at the center of Plaintiffs claims rely on their devices functioning as intended. *See WhatsApp*,. 472 F. Supp. 3d at 659–60 (dismissing trespass claim based on the installation of malware where the allegations demonstrated the malware relied on the plaintiff's servers functioning as intended). Consistent with California law, the Court should reject Plaintiffs' nonsensical effort to manufacture a trespass claim.

C. Statutory Larceny (Count 7)

Section 496(a) of the Penal Code, under which Plaintiffs' claim arises, concerns the intentional receipt or concealment of property the defendant knew to be stolen. That is not what Plaintiffs accuse Google of doing.[17] Rather, Plaintiffs accuse Google of "stealing" their information in the first instance under section 484 of the Penal Code. (*See* CAC ¶¶ 23, 412). "[T]he California statute making larceny a crime is declaratory of the common law and is therefore to be construed by application of common law principles." *People v. Davis*, 19 Cal. 4th

[17] Plaintiffs make the bare assertion that Google "concealed . . . Class Members' Health Information . . . ." (CAC ¶ 390). Other than making this recitation of an element of the offense, Plaintiffs provide no factual allegations to support this assertion. *Iqbal*, 556 U.S. at 678 (threadbare recitals of the cause of action insufficient). To the contrary, Plaintiffs point to a number of public disclosures (not to mention the Health Care Providers' own) that explain this data collection. Plaintiffs may have never had access to the subject data, but that does not mean Google "concealed" it; it simply means that it was never in Plaintiffs' possession to begin with and was, as a result, not their "property."

301, 313 (1998). Plaintiffs attempt to assert claims of theft by larceny and false pretenses, but fail to allege sufficient facts for either.

To state a claim for theft by larceny, Plaintiffs must show that Google (1) took possession; (2) of personal property; (3) owned or possessed by Plaintiffs; (4) by means of trespass; (5) with the intent to steal the property; and (6) carried away the property." *People v. Brock*, 143 Cal. App. 4th 1266, 1275 (2006). As discussed above, Google did not take any property owned or possessed by Plaintiffs, but instead allegedly obtained event data generated by the Websites. And since Plaintiffs cannot establish a tort of trespass, they cannot show that Google "stole" property "by means of trespass." *See Brock*, 143 Cal. App. 4th at 1275. "The intent to steal . . . is the intent, without a good faith claim of right, to permanently deprive the owner of possession." *Davis*, 19 Cal. 4th at 306. Here, Google has deprived Plaintiffs of nothing, permanently or otherwise.

Finally, the "carrying away" or "asportation" requirement demonstrates that larceny by theft concerns *tangible* property that one physically takes and "carries away." *See People v. Beaver*, 186 Cal. App. 4th 107, 122 (2010) (Theft by larceny "applies to situations where a defendant physically takes property from another's actual or constructive possession.")[18]

To state a claim for theft by false pretenses, the Plaintiffs must show "'(1) the defendant made a false pretense or representation to the owner of property; (2) with intent to defraud the owner of that property; and (3) the owner transferred the property to the defendant in reliance on the representation.'" *People v. Hartley*, 248 Cal. App. 4th 620, 627 (2016). Theft by false pretenses "involves a consensual transfer of title." *Boegman v. Smith*, 2018 WL 3140469, at *9 (S.D. Cal. June 27, 2018).

Plaintiffs cannot allege that Google made any false representation or pretense to them because they contend they were "unaware" of Google's use of cookies to obtain their data. CAC

[18] Cases applying this reasoning more directly are unpublished. *See, e.g.*, *People v. Nguyen*, 166 Cal. Rptr. 3d 295, 300 (Cal. App. Dec. 17, 2013) (unpublished) ("Given the 'carrying away' requirement, known as 'asportation,' it necessarily applies to theft of tangible items."); *also People v. Lawrence*, 2015 WL 9259196 (Cal. App. Dec. 17, 2015) ("The theft by larceny instruction . . . was not appropriate . . . because no physical property was taken . . . .").

¶¶ 435(c). Though unclear in the pleadings, it appears this theory may be based on Google's purported "disguising" certain cookies as "first-party cookies." *See, e.g.*, CAC ¶ 4. But rather than claiming Google falsely presents these cookies to Plaintiffs, Plaintiffs allege the cookies are simply placed in Plaintiffs' devices by Source Code "hidden in the website," "[a]lmost immediately upon visiting" a website. CAC ¶¶ 4, 40. As Plaintiffs allege that Google carried out the so-called "theft" through "hidden" software, they cannot legitimately claim to have transferred property to Google "in reliance on [any] representation" from Google. *Hartley*, 248 Cal. App. 4th at 627. Nor can Plaintiffs now plead that there has been a "consensual transfer of title," as this theory requires. *Boegeman*, 2018 WL 3140469, at *9.

Finally, because Plaintiffs have failed to establish that Google obtained property "in any manner constituting theft," it cannot show Google concealed property from the Plaintiffs "knowing the property to be so stolen." Cal. Penal Code § 496.

California law provides ample protection for privacy harms. Reference to property law in an effort to obtain treble damages is improper. *See Intel*, 30 Cal. 4th at 1361–62. Plaintiffs statutory larceny claim should be dismissed.[19]

D. California Comprehensive Data Access and Fraud Act (CDAFA) (Count 8)

Plaintiffs have no statutory standing to bring an action under CDAFA because they fail to allege any damage or loss. Cal. Penal Code § 502(e)(1). Additionally, Plaintiffs cannot show that Google was aware it lacked authorization for the complained-of conduct.

[19] Google is aware of one case upholding a statutory larceny claim involving personal data. *Calhoun*, 526 F. Supp. 3d at 635. That case considered only whether data could be deemed "property," and not whether the plaintiffs had satisfied the elements of statutory larceny. *See id.* (addressing argument that "'personal information' does not constitute property"). Further, *Calhoun*'s sole authority for the proposition that California recognizes a "property interest" in personal information did not hold that. *See CTC Real Estate Servs. v. Lepe*, 140 Cal. App. 4th 856, 860 (2006). *CTC* held that "personal identifying information" is a "valuable asset" that can be subject to theft, citing to *identity theft* statutes. *Id.* at 860 (citing Cal. Civ. Code § 1798.92(c); Cal. Penal Code § 530.5(b)). If section 484 already covered the theft of data, these identity theft statutes would be superfluous. *See Shoemaker v. Myers*, 52 Cal. 3d 1, 22 (1990) ("We do not presume that the Legislature performs idle acts . . ."). The sole larceny case *Calhoun* relied upon had nothing to do with personal data. *People v. Kwok*, 63 Cal. App. 4th 1236, 1248–49 (1998) (holding that the unauthorized copying of a key constitutes theft).

1. Standing under CDAFA

CDAFA permits a civil action only by a person "who suffers damage or loss by reason of a violation." Cal. Penal Code § 502(e)(1). Plaintiffs claim they suffered "damages and losses" including: (1) the inability of Plaintiffs to communicate with Health Care Providers; (2) damaged relationships with Health Care Providers; (3) resources expended to investigate and respond to Google's alleged violations; and (4) diminution of value of Plaintiffs' Health Information. (CAC ¶¶ 437–38). None of these "losses" support Plaintiffs' claim.

First, Plaintiffs' allegations contradict the assertion that Google disrupted Plaintiffs' ability to communicate with Health Care Providers. By Plaintiffs' own account, the alleged data acquisition can *only* occur when Plaintiffs communicate with the providers, and Plaintiffs allege they were unaware of the cookies. CAC ¶¶ 402, 435(c); *Kurowski*, 2023 WL 4707184, at *10.

Second, there is no authority that Plaintiffs' "damaged relationships" with or subjective feelings about their Health Care Providers constitutes a cognizable loss. *See Pratt v. Higgins, et al.*, 2023 WL 4564551, at *9 (N.D. Cal. July 17, 2023) (dismissing claim that accessing medical information gave rise to any cognizable loss under CDAFA).

Next, Plaintiffs' vague allegation that they expended resources to "investigate and respond to" the alleged violations is insufficient. Under the statute's plain terms, compensable investigation costs are limited to those "reasonably and necessarily incurred . . . to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." Cal. Penal Code § 502(e)(1). Whatever Plaintiffs may have done to "investigate and respond to" purported violations, Plaintiffs make no allegation that they investigated whether Google "altered, damaged, or deleted" their data, or that they incurred costs in the course of such an investigation.[20] Nor could Plaintiffs plausibly suggest they "reasonably and necessarily" incurred investigative costs to discover cookies and practices that both Google

[20] The only "investigation" Plaintiffs allege is the "the investigation of counsel." CAC ¶ 19. Holding that such legal costs are "damages and loss" within the meaning of section 502(e)(1) would render the legislature's separate allowance for attorneys' fees superfluous. Cal. Penal Code § 502(e)(2). If one could evade the "damage or loss" limitation simply by retaining counsel, there would be no lawsuit in which the "damage or loss" limitation has any effect.

and their Health Care Providers directly disclosed

Finally, courts have rejected Plaintiffs' "diminution of value" theory, particularly where, as here, the plaintiffs do not demonstrate that they were ready and willing to market their personal data. *See, e.g.*, *Cottle,* 536 F. Supp. 3d at 484; *Wesch*, 2021 WL 6206644, at *5; *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 149 (3d Cir. 2015). Plaintiffs thus cannot establish standing under CDAFA.

2. Plaintiffs Are Not "Owners" or "Lessees" of the Data

Plaintiffs' CDAFA claim also fails because they are not "owners" or "lessees" of the data. As discussed above (section VI.B.2), Plaintiffs do not own the event data generated by the Health Care Providers on their own websites; the Healthcare Providers, not Plaintiffs, create and have the right to control access to it. *See Alderson*, 718 F. Supp. 2d at 1197 (information was not "property" where the plaintiff did not have the right to exclude others from obtaining it).

3. Plaintiffs Cannot Establish Google Knew Its Collection was Unauthorized

While Plaintiffs assert that Google's alleged collection was unauthorized (*see* CAC ¶ 435), they fail to establish Google knew it acted without permission. "Absent indication of contrary purpose in the language or legislative history of the statutes, [courts] ordinarily read a phrase in a criminal statute that introduces the elements of a crime with the word 'knowingly' as applying that word to each element." *United States v. Olson*, 856 F.3d 1216, 1220 (9th Cir. 2017). Here, the elements of CDAFA, a criminal statute, are introduced with the word 'knowingly,' and there is no indication that the legislature intended to impose strict liability on individuals who accessed data under a good faith but mistaken belief of authorization. *See id.* Plaintiffs must not only allege that Google lacked permission, they must show Google *knew* it lacked permission. *See id.*

The closest Plaintiffs come is alleging that "Google's own policies prohibit Google from accessing and using Plaintiffs' and Class Members' Health Information." CAC ¶ 435. But that fact demonstrates that Google had all the less reason to know that Health Care Providers would send any PHI. While Plaintiffs assert that Google's Search infrastructure is capable of determining which categories of websites may implicate PHI (CAC ¶¶ 178–95), they also

contend Google "fails to use its systems to detect, deter, or prevent its collection of Health Information from Health Care Providers." (CAC ¶¶ 239, 474). Plaintiffs' allegations thus refute that Google knew it acted without authorization. *See In re A.L.*, 38 Cal. App. 5th 15, 21 (2019) (holding actual knowledge means subjective awareness of necessary facts).

E. Aiding and Abetting (Count 9)

Plaintiffs' aiding and abetting claim is unclear; it is not apparent what violation Google is alleged to have "aided and abetted." For instance, it appears Plaintiffs allege Google generally assisted Health Care Providers in "breaching their duty" to Plaintiffs under a slew of statutes and even the Hippocratic Oath. CAC ¶¶ 444–46. Plaintiffs then discuss their right to privacy under the California Constitution before appearing to assert direct liability claims. *See* CAC ¶ 457.

Aiding and abetting liability in California concerns intentional torts. *Yazdanpanah v. Sacramento Valley Mortg. Grp.*, 2009 WL 4573381, at *5 (N.D. Cal. Dec. 1, 2009). Courts do not recognize liability for aiding and abetting statutory violations unless the statute expressly provides for such liability. *See, e.g.*, *DuFour v. Be., LLC*, 2010 WL 431972, at *3–4 (N.D. Cal. Feb. 2, 2010) (rejecting argument that secondary liability is presumptively available for statutory violations); *Wynn v. NBC, Inc.*, 234 F. Supp. 2d 1067, 1113–14 (C.D. Cal. 2002) (dismissing aiding and abetting claim based on non-tort); *see also JBF Interlude 2009 Ltd. v. Quibi Holdings LLC*, 2020 WL 6203555, at *7 (same and collecting cases). Plaintiff's non-tort claims, such as statutory violations and purported oathbreaking, cannot support their aiding and abetting claim.

Google presumes that Plaintiffs found this claim on a violation of the California constitutional right of privacy—the only claim Plaintiffs address specifically. While Google has found no authority supporting aiding and abetting liability for constitutional violations, Plaintiffs ultimately fail to adequately plead a claim even assuming one exists.

To state a claim for aiding and abetting, Plaintiffs must establish an underlying tort by the Health Care Providers that is independent of the alleged "aiding and abetting." *See Richard B. Levine, Inc. v. Higashi*, 131 Cal. App. 4th 566, 574 (2005). This they cannot do.

Plaintiffs' constitutional claim relies on the application of California law to the relationship between Plaintiffs and their Health Care Providers, which Plaintiffs allege stems

from Google's contracts with those Health Care Providers for the use of its "Source Code." Even assuming those contracts call for application of California law to disputes between Google and those Health Care Providers, this does not establish that California law should govern the relationship between out-of-state providers and their out-of-state consumers. Indeed, where Plaintiffs' counsel brought claims against Health Care Providers for the same conduct at issue here, Plaintiffs brought their claims under the law of the state in which the Health Care Provider is situated. *See, e.g.*, *Kurowski*, 2023 WL 2349606, at *8–9 (asserting privacy claims under Illinois law regarding Illinois Health Care Provider's use of Google Analytics, among other products, which the court dismissed for failure to state a claim). The claims of all non-resident Plaintiffs thus fail at the outset.[21]

Plaintiffs have also failed to assert a claim on behalf of the California plaintiffs regarding their California providers. The reasoning Google provides above with regard to Plaintiffs' direct claim for invasion of privacy applies with greater force to these Health Care Providers. Kaiser's privacy policy could not have been clearer about the use of third-party cookies to collect activity data. *See* RJN Ex. 23. Plaintiffs thus could have no reasonable expectation of privacy as it relates to Kaiser's acquisition of their activities on Kaiser's website. Similarly, John Doe II and IV have failed to offer more than conclusory assertions about what information Kaiser collected. *See Cousin*, 2023 WL 4484441, at *3; *see also Kurowski*, 2023 WL 4707184, at *3, *8 (dismissing privacy claims brought by Plaintiffs' counsel for failure to allege the private data collected). Nor do Plaintiffs provide any reason to believe their Health Care Providers' access to their activity data—characterized as "communications" knowingly provided—constitutes a "serious intrusion." *See Kurowski*, 2023 WL 2023 , at *8 (healthcare website metadata "does not in the least bit fit" into the category of individually identifiable health information).

But even if Plaintiffs had sufficiently alleged an underlying tort, Plaintiffs must still demonstrate that Google knew of the wrongdoing and substantially assisted or encouraged it.

[21] This leaves John Doe II, John Doe IV, who are allegedly patients of Kaiser in California. Jane Doe VI, though a California resident, alleges that the relevant website is operated by Planned Parenthood Federation of America, which is not alleged to be headquartered or operating in California. (CAC ¶¶ 20, 22, 29).

Chetal v. Am. Home Mortg., 2009 WL 2612312, at *4 (N.D. Cal. Aug. 24, 2009). Plaintiffs offer nothing more than conclusory assertions to support this claim. As described above, there is no plausible explanation that Google even "knew" of the Health Care Providers' alleged misconduct, much less identify facts showing that Google had "control, influence or involvement" in the unlawful conduct—*i.e.*, the supposed invasion of privacy. *Decarlo v. Costco Wholesale Corp.*, 2020 WL 1332539, at *5–6 (S.D. Cal. Mar. 23, 2020).

F. Breach of Contract (Count 10)

Plaintiffs base their contract claim on Google's TOS and Privacy Policy. Those claims fail because the TOS and Privacy Policy apply by their plain terms to *Plaintiffs'* use of Google's services, not Plaintiffs' use of third-party services that may also use Google's services. Even assuming the TOS and Privacy Policy had any applicability here, Plaintiffs blatantly alter their text in the Complaint to suit their narrative.

1. Alleged Breach One

Plaintiffs first allege that Google broke a promise in its TOS that, according to Plaintiffs, Google would enforce applicable laws and its policies against third-parties. But the plain text of the TOS provided that *Plaintiffs* had to comply with all applicable laws. This term was a promise made by Plaintiffs, not Google. The same section makes clear that Plaintiffs' remedy for third-party violations was simply to report the violation to Google. RJN Ex. 14 at 4 ("If you find that others aren't following these rules, many of our services allow you to report abuse."). It is equally clear that Google made no promise to take action on such reports. *Id.* ("***If*** we act on a report of abuse . . .") (emphasis added). Plaintiffs' absurd reading would require Google to be a global enforcer of all laws applicable to any Google user.

2. Alleged Breach Two

Plaintiffs assert a variety of other purported breaches of Google's Privacy Policy. Plaintiffs claim Google breached a representation that Google collects health information "if you choose to provide it." But the information Plaintiffs' accuse here–pseudonymous event metadata concerning Plaintiffs' activity on healthcare websites—is not the "health information" described in Privacy Policy, which concerns the actual medical records or metrics about a specific person.

The *noscitur a sociis* canon provides that a word "takes meaning from the company it keeps." *People v. Drennan*, 84 Cal. App. 4th 1349, 1355 (2000). "In accordance with this principle of construction, a court will adopt a restrictive meaning of a listed item if acceptance of a more expansive meaning would . . . make the item markedly dissimilar to the other items in the list.'" *People ex rel. Lungren v. Superior Court*, 14 Cal.4th 294, 307 (1996)).

The "health information" referred to in the Privacy Policy includes "medical history, vital signs and health metrics (like blood glucose levels), and other similar information." RJN Ex. 19 at 17. "Health information," therefore, means *actual* medical history and metrics about a person, not the URLs and event data associated with a pseudonymous identifier that may, or may not, have any relation to health. *See Smith, See* 262 F. Supp. 3d at 954–55 (URLs for pages "containing information about treatment options for melanoma, information about a specific doctor, [or] search results related to the phrase 'intestine transplant'" are not PHI); *Kurowski*, 2023 WL 4707184, at *4 (browsing metadata on healthcare provider's website "does not in the least bit fit" into the category of individually identifiable health information covered by HIPAA). This is confirmed by the separate provision for collection of web activity, search terms, and other information on third party websites. Cal. Civ. Code § 1641 ("[T]he whole of a contract is to be taken together, so as to give effect to every part, if reasonably practicable, each clause helping to interpret the others."). Because "health information" as used in the Privacy Policy refers to actual medical information rather than web activity data from which assumptions may be made about a person, Plaintiffs' second theory of breach of contract fails.

Further, even if the "health information," as used in the Privacy Policy, was intended to cover web activity, Plaintiffs do not allege that Google circumvented or failed to honor the controls Google specifically identified in the Privacy Policy to control such data collection. *See In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 832–33 (N.D. Cal. 2020) (dismissing claim that Google breached Privacy Policy by sharing data without consent where Plaintiffs failed to address other circumstances enabling Google to share data). Google's Privacy Policy informs users that it collects web and app activity information, and that such data collection is addressed in the users' My Activity controls. RJN Ex. 19 at 17; *In re Google Assistant*, 457 F.

Supp. 3d at 833. No Plaintiff alleges that he or she has disabled the relevant settings, or that Google somehow circumvented those controls.

3. Alleged Breaches Three, Four, Five and Six

Plaintiffs' third, fourth, and fifth theories of breach claim that Google breaks its promise not to personalize advertisements based on Health Information, and to restrict advertisers in the same way. Plaintiffs' allegations fail to support this theory of breach, and none alleges he or she received a personalized advertisement based on PHI.

Aside from repeating the conclusory assertion that Google allows personalized advertisements based on personal health information (*see, e.g.*, CAC ¶¶ 111, 233), Plaintiffs' only factual allegations are off the mark. Plaintiffs identify Google's policies and restrictions that allow "healthcare-related advertising" in some circumstances. CAC ¶¶ 251–52. But Google does not promise to prohibit healthcare-related advertisements generally. It prohibits *personalized* advertisements based on *the users'* sensitive health data. CAC ¶¶ 250 Nos. 3–4. Google's Privacy Policy makes clear that "personalized ads" refers to advertising based on information Google collects about the user. RJN Ex. 19 at 6–7. (informing that Google uses "the information [it] collect[s]" about the user to personalize services, including ads). Because Plaintiffs' allegations go no further than suggesting Google permits generalized, non-personalized healthcare advertising, Plaintiffs third, fourth, fifth, and sixth theories of breach fail.

These theories fail for the additional reason that no Plaintiff alleges he or she ever saw a personalized advertisement based on their PHI (or even any generalized healthcare-related ads). Plaintiffs thus cannot show that *they* have suffered a breach, and they lack standing to assert a claim for the mere risk that they or someone else could see an offending advertisement. *See Cahen v. Toyota Motor Corp.*, 717 F. App'x 720, 724 (9th Cir. 2017) (affirming dismissal of contract and other claims based on a *risk* of hacking).

4. Alleged Breaches Five, Six, Eight, Nine, Ten, Eleven, and Twelve

Plaintiffs' fifth, sixth, and eighth through twelfth theories of breach concern documents purportedly "reference[d]" in Google's Privacy Policy. These "referenced" documents cannot form the basis of a contract claim because they were not incorporated into the Privacy Policy.

Rather, these were documents that one could find by following hyperlinks. These hyperlinks did not explicitly reference the documents, and were thus not incorporated by reference. *Rodriguez*, 2021 WL 6621070, at *4 (no incorporation by reference where Google linked to a document with a hyperlink reading "learn more here" but did not reference the document itself).

Plaintiffs' fifth and eighth theories of breach acknowledge that the hyperlink text does not reference the document in question. (CAC ¶ 472 No. 5 & No. 8). Plaintiffs allege in their sixth and ninth through twelfth theories that Google's Privacy Policy directly references certain other documents, but these documents are nowhere mentioned in the Privacy Policy. The Privacy Policy does not include the phrases "What happens if you violate our policies" (Nos. 6, 10 & 11), "Safeguarding your data" (No. 9), or "Legal requirements" (No. 12). RJN Ex. 19. Simply being linked somewhere in the Privacy Policy is insufficient. *Rodriguez*, 2021 WL 6621070, at *4.

5. Alleged Breach Seven

Plaintiffs assert that Google does not "use its systems" to prevent the purportedly "unlawful tracking, collection and disclosure" of their information, in violation of a purported promise to protect users from illegal activity. (CAC ¶¶ 472 No.7, 488). This is another manipulation of the Privacy Policy's plain text.

Plaintiffs quote from a portion of the Privacy Policy purporting to explain what data Google collects from *a user* and how Google uses *that user's data*. RJN Ex. 19 at 18. It is not a statement about Google's use of its "systems" or other technologies. Similarly, the portion Plaintiffs quote does not refer to the use of users' data to protect users, but rather the use of such data for Google's own purposes, such as to protect Google systems. The header above the quoted language—"[b]usiness purposes for which information may be used or disclosed"—makes this clear. *Id.*. This is consistent with all other provisions in the section, which focus on how Google uses data internally for its own "business purposes." *See* Cal Civ. Code § 1641 (a provision should be construed in light of the surrounding provisions). This provision cannot be read as an open-ended promise to users for Google to use "its systems" to protect against any "security threats, abuse, [or] illegal activity" they may encounter online.

G. Breach of Implied Contract (Counts 11 & 12)

Plaintiffs seek to assert a duplicative claim for breach of an implied contract between Google and its users. Because an express contract applies to these users, an implied contract claim is unavailable. *Hammerling*, 615 F. Supp. 3d at 1095–96. Plaintiffs also purport to assert an implied contract claim on behalf of those who do not have a Google Account, which is coextensive with the claims asserted on behalf of users, but fail to support any such claim.

"An implied contract is one, the existence and terms of which are manifested by conduct." Cal. Civ. Code § 1621. It is unclear what "conduct" Plaintiffs contend created the contract. For instance, Plaintiffs claim Google made "express promises," but an implied contract is, by definition, one in which "the agreement and promise have not been expressed in words." *Stanley v. Univ. S. Cal.*, 178 F.3d 1069, 1078 (9th Cir. 1999). Nor do Plaintiffs claim Google made these promises to non-users in any particular way, or that the non-users saw them, relied on them, or otherwise intended for these promises to form the basis for their agreement with Google. (*See* CAC ¶ 519(a)).[22] In these circumstances, Plaintiffs fail to establish a "*mutual agreement and intent*" necessary to support an implied contract. *Gorlach v. Sports Club Co.*, 209 Cal. App. 4th 1497, 1508 (2012) (emphasis in original).

Plaintiffs also point to their subjective expectations of privacy. (*Id.* ¶ 519(c)). But unilateral, subjective expectations fail to support an implied contract. *See Zenith Ins. Co. v. O'Connor*, 148 Cal. App. 4th 998, 1010 (2007).

Finally, Plaintiffs point to federal, state, and common law protections regarding Health Information. Statutes, however, are not private contracts, nor are they automatically incorporated into contracts. *See e.g.*, *Metzger v. Wells Fargo Bank, N.A.*, 2014 WL 1689278, at *7 (C.D. Cal. Apr. 28, 2014) ("With respect to the alleged failure by Wells Fargo to comply with Cal. Civ. Code §§ 2924.5 and 2923.6(c), an implied covenant is based on the terms of the contract, rather than statutory duties imposed."). In any event, because Plaintiffs have not established a breach of the express contract, their duplicative implied contract claim likewise fails.

[22] Indeed, insofar as an implied contract is defined by conduct, Plaintiffs contend Google's conduct was inconsistent with these promises. (*Id.* ¶¶ 525–531).

H. Breach of the Implied Covenant of Good Faith and Fair Dealing (Count 13)

Plaintiffs' last cause of action alleges a breach of the implied covenant of good faith by "intercepting their Health Information." (CAC ¶ 535). Because Plaintiffs allege that the express terms of their contract with Google covers the handling of their "Health Information," (*see* CAC ¶¶ 475–76, 489), they cannot assert an implied covenant claim for the same conduct. *See Careau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal. App. 3d 1371, 1395 (1990) ("If the allegations do not go beyond the statement of a mere contract breach and, relying on the same alleged acts, simply seek the same damages or other relief already claimed in a companion contract cause of action, they may be disregarded as superfluous as no additional claim is actually stated."). To the extent the handling of Health Information is not covered by the terms of the alleged contracts, the claim would still fail; the implied covenant cannot impose new contractual duties beyond those found in the contract. *Guz v. Bechtel Nat'l Inc.*, 24 Cal. 4th 317, 249 (2000).

I. Unjust Enrichment (Count 14)

An unjust enrichment claim is not a standalone claim under California law and is construed as a quasi-contract claim. *Saroya v. Univ. of the Pac.*, 503 F. Supp. 3d 986, 998 (N.D. Cal. 2020). Such a claim is inappropriate where, as alleged here, a valid, express contract covers the same subject matter. *Id.*; *Rutherford Holdings, LLC v. Plaza Del Rey*, 223 Cal. App. 4th 221, 231 (2014). Plaintiffs cannot maintain both contract and unjust enrichment actions "unless the plaintiff also pleads facts suggesting that the contract may be unenforceable or invalid," which Plaintiffs fail to do here. *Saroya*, 503 F. Supp. 3d at 998.

Further, despite the conclusory assertion that Plaintiffs lack an adequate remedy at law, they allege a host of legal claims seeking the same relief—the value of their data. *See, e.g.*, CAC ¶¶ 460, 530(d)–(e); 528(e); *see also Sonner v. Premier Nutrition Corp.*, 917 F.3d 834, 844 (9th Cir. 2020) (affirming dismissal of unjust enrichment claim where plaintiff sought the same relief in equitable restitution as in damages).

Plaintiffs unjust enrichment claim should be dismissed.

VII. CONCLUSION

This Court should deny Plaintiffs' Motion and dismiss each of Plaintiffs' claims.

Dated: August 3, 2023

WILLKIE FARR & GALLAGHER LLP

By: */s/ Benedict Hur*

BENEDICT HUR
SIMONA AGNOLUCCI
EDUARDO SANTACANA
TIFFANY LIN

Attorneys for Defendant Google LLC